【TITLE OF THE INVENTION】

鍵共有システム、共有鍵生成装置及び共有鍵復元装置

KEY AGREEMENT SYSTEM, SHARED-KEY GENERATION APPARATUS, AND SHARED-KEY RECOVERY APPARATUS

【BACKGROUND OF THE INVENTION】

【(1) Field of the Invention】

本発明は、情報セキュリティ技術としての暗号技術に関し、特に、第三者に知られることなく、鍵を配送する技術に関する。

【(2) Description of the Related Art】

従来より、送信装置から受信装置へ情報を秘密に送信するために、公開鍵暗号方式が用いられる。

公開鍵暗号方式では、送信装置は、通信内容を受信装置の公開鍵を用いて暗号化して送信し、受信装置は、暗号化された通信内容を受信し、受信した通信内容を自身の秘密鍵を用いて復号して元の通信内容を得る。(例えば、非特許文献１参照)。

１９９６年、高速処理が可能な公開鍵暗号として、ＮＴＲＵ暗号が提案された（例えば、非特許文献２参照)。ＮＴＲＵ暗号では、高速に演算可能な多項式演算を用いて暗号化と復号化とを行うので、べき乗演算を行うＲＳＡ暗号や楕円曲線上の点のスカラ倍演算を行う楕円曲線暗号と比較すると、これら従来の公開鍵暗号よりもソフトウェアにより高速に処理することが可能である。

しかし、このＮＴＲＵ暗号では、公開鍵を用いて平文を暗号化して暗号文を生成し、正規の秘密鍵を用いて暗号文を復号して復号文を生成する際に、復号文が元の平文と異なる場合が発生する。このことを復号エラーが発生するという。なお、復号エラーを回避する方法として、平文に付加情報を付加して暗号化し、平文のハッシュ関数値と共に送信する方法が開示されている（例えば、特許文献１参照)。

一方で、近年、公開鍵暗号の新しい概念として、鍵カプセル化メカニズム（Ｋｅｙ　Ｅｎｃａｐｓｕｌａｔｉｏｎ　Ｍｅｃｈａｎｉｓｍｓ）と呼ばれる方式が提案されている（例えば、非特許文献３参照)。この鍵カプセル化メカニズムは、公開鍵暗号を用いて送信装置と受信装置との間で共有鍵を配送するアルゴリズムであり、送信装置は、暗号化アルゴリズムＥに受信者の公開鍵ｐｋを入力して暗号文Ｃと共有鍵Ｋを生成し、暗号文Ｃを受信装置に伝送する。次に、受信装置は、復号アルゴリズムＤに、秘密鍵ｓｋと暗号文Ｃを入力して送信装置と同じ共有鍵Ｋを求める。

このようにして鍵カプセル化メカニズムを用いて共有鍵Ｋを送信装置と受信装置とで共有した後に、送信装置は、受信装置へ送信すべき平文を、共有鍵Ｋを用いて共通鍵暗号方式に

より暗号化して暗号文を生成し、生成した暗号文を受信装置へ送信する。受信装置は、暗号文を受信し、受信した暗号文を共有鍵Ｋを用いて前記共通鍵暗号方式により復号して復号文を生成する。

鍵カプセル化メカニズムでは、送信者から受信者に一方的に情報の送信が行われていながら、送信者が作為的に共有鍵を作成できず、送信者による不正が抑制されている点が従来にない特徴である。

このような鍵カプセル化メカニズムとして、ＰＳＥＣ－ＫＥＭと呼ばれるアルゴリズムが開示されている（例えば非特許文献３、非特許文献４参照）。以下に、非特許文献４に記載されているＰＳＥＣ－ＫＥＭアルゴリズムについて説明する。

（１）ＰＳＥＣ－ＫＥＭのシステムパラメータ

ＰＳＥＣ－ＫＥＭは、以下のシステムパラメータを持つ。

・楕円曲線：Ｅ

・楕円曲線上の位数ｎの点：Ｐ

・ハッシュ関数：Ｇ、Ｈ

なお、楕円曲線、位数及びハッシュ関数については、非特許文献１に詳細が記述されているので、ここでは説明を省略する。

（２）ＰＳＥＣ－ＫＥＭの公開鍵と秘密鍵

・ランダムにＺｎの要素ｘを選び、Ｗ＝ｘ＊Ｐを生成する。

ここで、Ｚｎは、{０，１，．．．．，ｎ－１}からなる集合であり、ｘ＊Ｐは、楕円曲線上の点Ｐをｘ個、加算することにより得られる楕円曲線上の点を表す。なお、楕円曲線上の点の加算方法については、非特許文献１に記述されている。

・公開鍵ｐｋを（Ｅ，Ｐ，Ｗ，ｎ）とし、秘密鍵ｓｋをｘとする。

（３）ＰＳＥＣ－ＫＥＭの暗号化

暗号化時には、以下に述べる暗号化アルゴリズムＫｅｍＥに公開鍵ｐｋを入力して共有鍵Ｋと暗号文Ｃを出力する。以下に暗号化アルゴリズムＫｅｍＥについて説明する。

・ハッシュ関数Ｈの出力ビット長と同じ長さのｓをランダムに生成する。

・Ｇ（ｓ）を生成し、Ｇ（ｓ）を分割して、ａとＫとを生成する。ａは、Ｇ（ｓ）の上位複数ビットからなるビット列であり、Ｋは、残りのビットからなるビット列である。ここで、Ｇ（ｓ）＝ａ｜｜Ｋである。「｜｜」は、ビット結合を表す演算子である。つまり、ａとＫとを結合すると、Ｇ（ｓ）が得られる。

・Ｒ＝ａ＊Ｐ、Ｑ＝ａ＊Ｗを生成する。

・ｖ＝ｓ　ｘｏｒ　Ｈ（Ｒ｜｜Ｑ）を生成する。ここで、ｘｏｒは排他的論理和演算を表す。

・共有鍵Ｋと暗号文Ｃ＝（Ｒ，ｖ）を出力する。

（4）ＰＳＥＣ－ＫＥＭの復号化

復号化時には、以下に述べる復号アルゴリズムＫｅｍＤに暗号文Ｃ＝（Ｒ，ｖ）と公開鍵ｐｋと秘密鍵ｓｋを入力して共有鍵Ｋを出力する。以下に復号アルゴリズムＫｅｍＤについて説明する。

・Ｑ＝ｘ＊Ｒを生成する。

・ｓ＝ｖ　ｘｏｒ　Ｈ（Ｒ｜｜Ｑ）を生成する。

・Ｇ（ｓ）を生成し、Ｇ（ｓ）をＧ（ｓ）＝ａ｜｜Ｋと分割する。

・Ｒ＝ａ＊Ｐが成立するかどうかチェックする。成立すれば共有鍵Ｋを出力する。

このＰＳＥＣ－ＫＥＭアルゴリズムを、送信装置と受信装置の間で暗号化通信を行う暗号システムに応用する場合、まず、送信装置は、通信先受信装置の公開鍵ｐｋを取得し、取得した公開鍵ｐｋを前述の暗号化アルゴリズムＫｅｍＥに入力して共有鍵Ｋと暗号文Ｃを導出して、暗号文Ｃを受信装置へ送信する。

次に、受信装置は、送信装置から暗号文Ｃを受信し、受信した暗号文Ｃと自身が有する公開鍵ｐｋ・秘密鍵ｓｋを前述の復号アルゴリズムＫｅｍＤに入力して、送信装置が導出したものと等しい共有鍵Ｋを導出する。

以下に、さらに詳細に説明する。

今、ＰＳＥＣ－ＫＥＭアルゴリズムは、ハッシュ関数Ｈの入力を（ａ＊Ｐ｜｜ａ＊Ｗ）としており、暗号化アルゴリズムＫｅｍＥで、ランダムに生成した要素ｓにＨ（ａ＊Ｐ｜｜ａ＊Ｗ）の値を作用させてｖを生成する。そして、復号アルゴリズムＫｅｍＤでは、Ｒ＝ａ＊Ｐから秘密鍵ｓｋ（＝ｘ）を用いてＱ＝ｘ＊Ｒ＝ｘ＊（ａ＊Ｐ）＝ａ＊（ｘ＊Ｐ）＝ａ＊Ｗを求めることができるので、ｖにＨ（ａ＊Ｐ｜｜ａ＊Ｗ）の値を作用させて、暗号化アルゴリズムＫｅｍＥにおいて生成されたランダムな要素ｓを求めることができる。

従って、暗号化アルゴリズムＫｅｍＥと復号アルゴリズムＫｅｍＤは、ハッシュ関数Ｇに同じｓの値を入力することができ、同じ共有鍵Ｋを導出することができる。この結果、秘密鍵ｓｋを有する受信装置は、送信装置が導出したものと同じ共有鍵Ｋを導出できることになる。

一方で、秘密鍵ｓｋを知らない他の受信装置は、たとえ公開鍵ｐｋを取得して暗号文Ｃを受信したとしても、秘密鍵ｓｋ（＝ｘ）を知らないのでＲ＝ａ＊ＰからＱ＝ａ＊Ｗ（＝（ａｘ）＊Ｐ）を計算できず、送信装置が導出したものと同じ共有鍵Ｋを導出できない。

なぜならば、秘密鍵ｓｋを知らない他の受信装置は、公開鍵ｐｋしか利用できないので、上記Ｑの計算には秘密鍵ｓｋ（＝ｘ）の代わりに公開鍵ｐｋのＷ＝ｘ＊Ｐを利用することになるが、一般に、ａ＊ＰとＷ＝ｘ＊Ｐから、Ｑ＝ａ＊Ｗ（＝（ａｘ）＊Ｐ）を求めることは、楕円曲線上のＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題と呼ばれ、ａやｘの値を知らない限り計算困難だからである（例えば、非特許文献５参照）。

すなわち、ＰＳＥＣ－ＫＥＭアルゴリズムは、秘密鍵を用いずにａ＊Ｐからａ＊Ｗを計算することが困難なＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題を用いて、最終的に共有鍵Ｋを導出することにより、秘密鍵を知らなければその共有鍵Ｋを導出できないようにしている。

以上により、送信装置と受信装置とは、共有鍵Ｋを秘密に共有することができ、この後、秘密鍵暗号を用いて、送信装置から受信装置へ通信される通信内容データを、共有鍵Ｋを用いて共通鍵暗号で暗号化する。

（特許文献１）

特開２００２－２５２６１１号公報

（非特許文献１）

岡本龍明、山本博資、「現代暗号」、シリーズ／情報科学の数学、産業図書、1997.

（非特許文献２）

Jeffery Hoffstein, Jill Pipher, and Joseph H. Silverman, " NTRU: A ring based public key cryptosystem", Lecture Notes in Computer Science, 1423, pp.267-288, Springer-Verlag, 1998.

（非特許文献３）

Victor Shoup, " A proposal for an ISO standard for public key encryption (version 2.1)"、[online]、2001年12月20日、[2002年9月29日検索]、インターネット<URL: http://shoup.net/papers/iso-2_1.pdf>

（非特許文献４）

Tatsuaki Okamoto, " Generic conversions for constructing IND-CCA2 public-key encryption in the random oracle model"、[online]、The 5th Workshop on Elliptic Curve Cryptography(ECC 2001)、2001年10月30日、[2002年９月29日検索]、インターネット<URL: http://www.cacr.math.uwaterloo.ca/conferences/2001/ecc/okamoto.ppt>

（非特許文献５）

Neal Koblitz, " Algebraic Aspects of Cryptography", Algorithms and Computation in Mathematics Vol.3, pp.132-133, Springer-Verlag, 1998.

（発明が解決しようとする課題）

上述したように、従来のＰＳＥＣ－ＫＥＭアルゴリズムは、ハッシュ関数Ｈの入力にａ＊Ｐ，ａ＊Ｗを用い、秘密鍵を用いずにａ＊Ｐからａ＊Ｗを計算することが困難なＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題を用いて、最終的に共有鍵Ｋを導出することにより、秘密鍵を知らなければその共有鍵Ｋを導出できないようにしている。

しかしながら、ＮＴＲＵ暗号をはじめ、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題を利用しない他の公開鍵暗号には、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題のａ＊Ｐ、ａ＊Ｗに相当するもの

がないため、ＰＳＥＣ－ＫＥＭアルゴリズムを適用できない。すなわち、高速処理が可能なＮＴＲＵ暗号は、鍵カプセル化メカニズムであるＰＳＥＣ－ＫＥＭアルゴリズムを適用して共有鍵の配送を行うことができず、従って、送信装置と受信装置とは、その共有鍵を用いた送信装置から受信装置への暗号化通信ができないという問題点がある。

【SUMMARY OF THE INVENTION】

そこで、本発明は上記の問題点を解決するために、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題を利用しない暗号化方式を用いる場合であっても、共有鍵生成装置から共有鍵復元装置へ第三者に知られることなく共有鍵を配送し、この際に、共有鍵生成装置と共有鍵復元装置との間で異なる共有鍵が導出されるのを防止できる鍵共有システム、共有鍵生成装置、共有鍵復元装置、共有鍵生成方法、共有鍵復元方法、共有鍵生成プログラム及び共有鍵復元プログラムを提供することを目的とする。

上記目的を達成するために、本発明は、第３者に知られることなく共有鍵を生成する共有鍵生成装置及び共有鍵復元装置から構成される鍵共有システムであって、前記共有鍵生成装置は、シード値を生成するシード値生成手段と、生成された前記シード値から検証値及び共有鍵を生成する第１共有鍵生成手段と、生成された前記検証値を暗号化して、第１暗号化情報を生成する第１暗号化手段と、生成された前記検証値に基づいて、生成された前記シード値を暗号化して、第２暗号化情報を生成する第２暗号化手段と、生成された前記第１暗号化情報及び前記第２暗号化情報を送信する送信手段とを備え、前記共有鍵復元装置は、前記第１暗号化情報及び前記第２暗号化情報を受信する受信手段と、受信された前記第１暗号化情報を復号して第１復号検証値を生成する第１復号手段と、生成された前記第１復号検証値に基づいて、受信された前記第２暗号化情報を復号して、復号シード値を生成する第２復号手段と、前記第１共有鍵生成手段と同一の方法により、生成された前記復号シード値から第２復号検証値及び復号共有鍵を生成する第２共有鍵生成手段と、生成された前記第１復号検証値及び前記第２復号検証値に基づいて、生成された前記復号共有鍵を出力するか否かを判断する判断手段と、出力すると判断される場合に、生成された前記復号共有鍵を出力する出力手段とを備える。

この構成によると、前記共有鍵生成装置は、シード値から検証値及び共有鍵を生成し、前記検証値を暗号化して第１暗号化情報を生成し、前記検証値に基づいて、前記シード値を暗号化して第２暗号化情報を生成し、前記共有鍵復元装置は、前記第１暗号化情報を復号して第１復号検証値を生成し、前記第１復号検証値に基づいて、前記第２暗号化情報を復号して、復号シード値を生成し、前記共有鍵生成装置と同様にして、前記復号シード値から第２復号検証値及び復号共有鍵を生成し、生成された前記第１復号検証値及び前記第２復号検証値に基づいて、生成された前記復号共有鍵を出力するか否かを判断するので、共有鍵生成装置か

ら共有鍵復元装置へ第三者に知られることなく共有鍵を配送できると共に、この際に、共有鍵生成装置と共有鍵復元装置との間で異なる共有鍵が導出されるのを防止できるという効果がある。

ここで、前記共有鍵生成装置は、さらに、コンテンツを取得する取得手段と、生成された前記共有鍵を用いて、取得されたコンテンツを暗号化して、暗号化コンテンツを生成する暗号化手段とを備え、前記送信手段は、さらに、生成された前記暗号化コンテンツを送信し、前記受信手段は、さらに、前記暗号化コンテンツを受信し、前記共有鍵復元装置は、さらに、出力された前記復号共有鍵を用いて、受信された前記暗号化コンテンツを復号して、復号コンテンツを生成する復号手段と、生成された復号コンテンツを出力する出力手段とを備える。

この構成によると、共有鍵生成装置は、生成された前記共有鍵を用いて、取得されたコンテンツを暗号化して、暗号化コンテンツを生成し、前記共有鍵復元装置は、出力された前記復号共有鍵を用いて、受信された前記暗号化コンテンツを復号して、復号コンテンツを生成するので、第三者に知られることなく、共有鍵生成装置から共有鍵復元装置へコンテンツを送信することができるという効果がある。

また、本発明は、第３者に知られることなく共有鍵を相手の装置へ伝える共有鍵生成装置であって、シード値を生成するシード値生成手段と、生成された前記シード値から検証値及び共有鍵を生成する共有鍵生成手段と、生成された前記検証値を暗号化して、第１暗号化情報を生成する第１暗号化手段と、生成された前記検証値に基づいて、生成された前記シード値を暗号化して、第２暗号化情報を生成する第２暗号化手段と、生成された前記第１暗号化情報及び前記第２暗号化情報を送信する送信手段とを備える。

この構成によると、共有鍵生成装置は、検証値を暗号化して第１暗号化情報を生成し、前記検証値に基づいて、シード値を暗号化して第２暗号化情報を生成するので、二重の暗号化により、より安全性を高めることができるという効果がある。不正な第三者は、第１及び第２暗号化手段による２種の暗号化を知っていなければ、共有鍵を得ることはできない。

ここで、前記シード値生成手段は、乱数を生成し、生成した乱数を前記シード値とすることにより、前記シード値を生成する。

この構成によると、共有鍵生成装置は、乱数を生成し、生成した乱数を前記シード値とするので、シード値を生成し、検証値及び共有鍵を生成し、第１暗号化情報及び第２暗号化情報を生成し、第１暗号化情報及び第２暗号化情報を送信した後、次に、シード値を生成する際に、最初に生成されたシード値とは異なるように、後のシード値を生成することができる。従って、共有鍵生成装置により送信される第１暗号化情報及び第２暗号化情報は、毎回異なるものとなる。このため、不正な第三者が、共有鍵生成装置から相手の装置へ送信される第１暗号化情報及び第２暗号化情報をその都度、盗聴し、記録したとしても、記録している各第１暗号化情報及び第２暗号化情報から元のシード値を類推することは困難である。

ここで、前記共有鍵生成手段は、前記シード値に一方向性関数を施して関数値を生成し、生成した前記関数値から前記検証値及び前記共有鍵を生成する。

この構成によると、前記シード値に一方向性関数を施して、前記検証値を生成するので、前記検証値を第三者が知り得たとしても、前記検証値から前記シード値を求めることは困難である。このため、前記検証値からシード値を求め、さらに、共有鍵を求めることは事実上不可能である。

ここで、前記共有鍵生成手段は、前記シード値に、前記一方向性関数として、ハッシュ関数を施して前記関数値を生成する。

この構成によると、前記一方向性関数は、ハッシュ関数であるので、その演算アルゴリズムがよく知られており、適用が容易である。

ここで、前記共有鍵生成手段は、生成された前記関数値の一部を前記検証値とし、他の一部を前記共有鍵とすることにより、前記検証値及び前記共有鍵を生成する。

この構成によると、前記関数値の一部を前記検証値とし、他の一部を前記共有鍵とするので、前記検証値及び前記共有鍵の生成が容易である。

ここで、前記共有鍵生成手段は、前記シード値に一方向性関数を施して関数値を生成し、生成した前記関数値から前記検証値、前記共有鍵及びブラインド値を生成する。

この構成によると、前記シード値に一方向性関数を施して、前記検証値を生成するので、前記検証値を第三者が知り得たとしても、前記検証値から前記シード値を求めることは困難である。このため、前記検証値からシード値を求め、さらに、共有鍵を求めることは事実上不可能である。

ここで、前記第１暗号化手段は、公開鍵を取得する公開鍵取得部と、取得された前記公開鍵及び生成された前記ブラインド値を用いて、前記検証値に公開鍵暗号化アルゴリズムを施して前記第１暗号化情報を生成する公開鍵暗号化部と含む。

また、前記第１暗号化手段は、公開鍵を取得する公開鍵取得部と、取得された前記公開鍵を用いて、前記検証値に公開鍵暗号化アルゴリズムを施して前記第１暗号化情報を生成する公開鍵暗号化部と含む。

この構成によると、第１暗号化手段は、公開鍵暗号方式を用いるので、共有鍵暗号方式を用いる場合と比較すると、鍵の管理が容易である。

ここで、前記公開鍵暗号化アルゴリズムは、ＮＴＲＵ暗号方式によるものであり、前記公開鍵取得部は、前記公開鍵として、ＮＴＲＵ暗号方式の鍵生成アルゴリズムにより生成された公開鍵多項式を取得し、前記公開鍵暗号化部は、前記検証値から検証値多項式を生成し、前記ブラインド値からブラインド値多項式を生成し、ＮＴＲＵ暗号方式の暗号化アルゴリズムにより、前記公開鍵多項式を鍵として用い、前記検証値多項式を攪乱するために前記ブラインド値多項式を用いて、前記検証値多項式を暗号化して、多項式としての前記第１暗号化

情報を生成する。

また、前記公開鍵暗号化アルゴリズムは、ＮＴＲＵ暗号方式によるものであり、前記公開鍵取得部は、前記公開鍵として、ＮＴＲＵ暗号方式の鍵生成アルゴリズムにより生成された公開鍵多項式を取得し、前記公開鍵暗号化部は、前記検証値から検証値多項式を生成し、ブラインド値を生成し、生成した前記ブラインド値からブラインド値多項式を生成し、ＮＴＲＵ暗号方式の暗号化アルゴリズムにより、前記公開鍵多項式を鍵として用い、前記検証値多項式を攪乱するために前記ブラインド値多項式を用いて、前記検証値多項式を暗号化して、多項式としての前記第１暗号化情報を生成する。

この構成によると、ＮＴＲＵ暗号を採用することができる。

ここで、前記第２暗号化手段は、前記検証値に一方向性関数を施して関数値を生成し、生成した前記関数値を用いて、前記シード値に暗号化アルゴリズムを施して前記第２暗号化情報を生成する。

この構成によると、前記検証値に一方向性関数を施して得られた関数値を用いて、前記シード値に暗号化アルゴリズムを施して前記第２暗号化情報を生成するので、不正な第三者は、少なくとも、前記一方向性関数及び前記暗号化アルゴリズムを知っていなければ、前記第２暗号化情報から前記シード値を得ることはできない。

ここで、前記第２暗号化手段は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして排他的論理和を施すことにより、前記第２暗号化情報を生成する。

この構成によると、前記暗号化アルゴリズムは、排他的論理和であるので、演算が容易である。また、逆演算が可能である。

ここで、前記第２暗号化手段は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして共通鍵暗号化アルゴリズムを施すことにより、前記第２暗号化情報を生成する。

この構成によると、前記暗号化アルゴリズムは、共通鍵暗号化アルゴリズムであるので、よく知られており、適用が容易である。また、逆演算が可能である。

ここで、前記第２暗号化手段は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして加算を施すことにより、前記第２暗号化情報を生成する。

この構成によると、前記暗号化アルゴリズムは、加算であるので、演算が容易である。また、逆演算が可能である。

ここで、前記第２暗号化手段は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして乗算を施すことにより、前記第２暗号化情報を生成する。

この構成によると、前記暗号化アルゴリズムは、乗算であるので、演算が容易である。また、逆演算が可能である。

ここで、前記第２暗号化手段は、前記検証値に、前記一方向性関数としてハッシュ関数を

施して前記関数値を生成する。

この構成によると、前記一方向性関数は、ハッシュ関数であるので、その演算アルゴリズムがよく知られており、適用が容易である。

ここで、前記第２暗号化手段は、前記検証値を用いて、前記シード値に暗号化アルゴリズムを施して第２暗号化情報を生成する。

この構成によると、前記検証値を用いて、前記シード値に暗号化アルゴリズムを施すので、演算が単純であり、適用が容易である。

ここで、前記第２暗号化手段は、前記検証値及び前記第１暗号化情報を用いて、前記シード値を暗号化する。

この構成によると、前記検証値及び前記第１暗号化情報を用いて、前記シード値を暗号化するので、不正な第三者は、前記検証値及び前記第１暗号化情報を知らなければ、シード値を得ることができず、安全性が高まる。

ここで、前記第２暗号化手段は、前記検証値及び前記第１暗号化情報に一方向性関数を施して関数値を生成し、生成した前記関数値を用いて、前記シード値に暗号化アルゴリズムを施して前記第２暗号化情報を生成する。

この構成によると、一方向性関数と暗号化アルゴリズムとを用いるので、不正な第三者は、第１暗号化情報及び第２暗号化情報を知っていても、少なくとも一方向性関数と暗号化アルゴリズムとを知らなければ、シード値を得ることができず、安全性が高まる。

ここで、前記第２暗号化手段は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして排他的論理和を施すことにより、前記第２暗号化情報を生成する。

この構成によると、前記暗号化アルゴリズムは、排他的論理和であるので、演算が容易である。また、逆演算が可能である。

ここで、前記共有鍵生成装置は、さらに、コンテンツを取得する取得手段と、生成された前記共有鍵を用いて、取得されたコンテンツを暗号化して、暗号化コンテンツを生成する暗号化手段とを備え、前記送信手段は、さらに、生成された前記暗号化コンテンツを送信する。

この構成によると、共有鍵生成装置は、第三者に知られることなく、コンテンツを相手の装置へ送信することができる。

ここで、第３者に知られることなく共有鍵生成装置から共有鍵を受け取る共有鍵復元装置であって、前記共有鍵生成装置は、シード値を生成し、生成された前記シード値から検証値及び共有鍵を生成し、生成された前記検証値を暗号化して、第１暗号化情報を生成し、生成された前記検証値に基づいて、生成された前記シード値を暗号化して、第２暗号化情報を生成し、生成された前記第１暗号化情報及び前記第２暗号化情報を送信し、前記共有鍵復元装置は、前記第１暗号化情報及び前記第２暗号化情報を受信する受信手段と、受信された前記第１暗号化情報を復号して第１復号検証値を生成する第１復号手段と、生成された前記第１

復号検証値に基づいて、受信された前記第２暗号化情報を復号して、復号シード値を生成する第２復号手段と、前記共有鍵生成装置と同一の方法により、生成された前記復号シード値から第２復号検証値及び復号共有鍵を生成する共有鍵生成手段と、生成された前記第１復号検証値及び前記第２復号検証値に基づいて、生成された前記復号共有鍵を出力するか否かを判断する判断手段と、出力すると判断される場合に、生成された前記復号共有鍵を出力する出力手段とを備える。

この構成によると、共有鍵生成装置から第三者に知られることなく共有鍵を受信できると共に、この際に、共有鍵生成装置と共有鍵復元装置との間で異なる共有鍵が導出されるのを防止できるという効果がある。

ここで、前記共有鍵生成装置は、公開鍵を取得し、取得された前記公開鍵を用いて、前記検証値に公開鍵暗号化アルゴリズムを施して前記第１暗号化情報を生成し、前記第１復号手段は、前記公開鍵に対応する秘密鍵を取得する秘密鍵取得部と、取得された前記秘密鍵を用いて、受信した前記第１暗号化情報に、前記公開鍵暗号化アルゴリズムに対応する公開鍵復号アルゴリズムを施して前記第１復号検証値を生成する公開鍵復号部と含む。

この構成によると、第１復号手段は、公開鍵暗号方式を用いるので、共有鍵暗号方式を用いる場合と比較すると、鍵の管理が容易である。

ここで、前記公開鍵暗号化アルゴリズム及び前記公開鍵復号アルゴリズムは、ＮＴＲＵ暗号方式によるものであり、前記共有鍵生成装置は、前記公開鍵として、ＮＴＲＵ暗号方式の鍵生成アルゴリズムにより生成された公開鍵多項式を取得し、前記検証値から検証値多項式を生成し、ブラインド値を生成し、生成した前記ブラインド値からブラインド値多項式を生成し、ＮＴＲＵ暗号方式の暗号化アルゴリズムにより、前記公開鍵多項式を鍵として用い、前記検証値多項式を攪乱するために前記ブラインド値多項式を用いて、前記検証値多項式を暗号化して、多項式としての前記第１暗号化情報を生成し、前記受信手段は、多項式としての前記第１暗号化情報を受信し、前記秘密鍵取得部は、前記秘密鍵として、ＮＴＲＵ暗号方式の鍵生成アルゴリズムにより生成された秘密鍵多項式を取得し、前記公開鍵復号部は、ＮＴＲＵ暗号方式の前記暗号化アルゴリズムに対応する復号アルゴリズムにより、前記秘密鍵多項式を鍵として用いて、多項式としての前記第１暗号化情報を復号して、復号検証値多項式を生成し、生成した前記復号検証値多項式から前記第１復号検証値を生成する。

この構成によると、ＮＴＲＵ暗号を採用することができる。

ここで、前記共有鍵生成装置は、前記検証値に一方向性関数を施して関数値を生成し、生成した前記関数値を用いて、前記シード値に暗号化アルゴリズムを施して前記第２暗号化情報を生成し、前記第２復号手段は、生成された前記第１復号検証値に、前記一方向性関数を施して復号関数値を生成し、生成した前記復号関数値を用いて、受信された前記第２暗号化情報に、前記暗号化アルゴリズムに対応する復号アルゴリズムを施して前記復号シード値を

生成する。

この構成によると、第２復号手段は、一方向性関数及び復号アルゴリズムの２段階による演算方法を採用しているので、不正な第三者は、第１暗号化情報及び第２暗号化情報を知っていても、少なくとも一方向性関数と復号アルゴリズムとを知らなければ、シード値を得ることができず、安全性が高まる。

ここで、前記共有鍵生成装置は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして排他的論理和を施すことにより、前記第２暗号化情報を生成し、前記第２復号手段は、生成した前記復号関数値と前記第２暗号化情報とに、前記復号アルゴリズムとして排他的論理和を施すことにより、前記復号シード値を生成する。

この構成によると、前記復号アルゴリズムは、排他的論理和であるので、演算が容易である。また、前記暗号化アルゴリズムの逆演算である。

ここで、前記共有鍵生成装置は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして共通鍵暗号化アルゴリズムを施すことにより、前記第２暗号化情報を生成し、前記第２復号手段は、生成した前記復号関数値と前記第２暗号化情報とに、前記復号アルゴリズムとして、前記共通鍵暗号化アルゴリズムに対応する共通鍵復号アルゴリズムを施すことにより、前記復号シード値を生成する。

この構成によると、前記復号アルゴリズムは、共有鍵復号アルゴリズムであるので、よく知られており、適用が容易である。また、前記暗号化アルゴリズムの逆演算である。

ここで、前記共有鍵生成装置は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして加算を施すことにより、前記第２暗号化情報を生成し、前記第２復号手段は、生成した前記復号関数値と前記第２暗号化情報とに、前記復号アルゴリズムとして、減算を施すことにより、前記復号シード値を生成する。

この構成によると、前記復号アルゴリズムは、減算であるので、演算が容易である。また、前記暗号化アルゴリズムの逆演算である。

ここで、前記共有鍵生成装置は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして乗算を施すことにより、前記第２暗号化情報を生成し、前記第２復号手段は、生成した前記復号関数値と前記第２暗号化情報とに、前記復号アルゴリズムとして、除算を施すことにより、前記復号シード値を生成する。

この構成によると、前記復号アルゴリズムは、除算であるので、演算が容易である。また、前記暗号化アルゴリズムの逆演算である。

ここで、前記共有鍵生成装置は、前記検証値に、前記一方向性関数としてハッシュ関数を施して前記関数値を生成し、前記第２復号手段は、生成された前記第１復号検証値に、前記一方向性関数として前記ハッシュ関数を施して前記復号関数値を生成する。

この構成によると、前記一方向性関数は、ハッシュ関数であるので、その演算アルゴリズ

ムがよく知られており、適用が容易である。

ここで、前記共有鍵生成装置は、前記検証値を用いて、前記シード値に暗号化アルゴリズムを施して第２暗号化情報を生成し、前記第２復号手段は、生成された前記第１復号検証値を用いて、前記第２暗号化情報に、前記暗号化アルゴリズムに対応する復号アルゴリズムを施して、前記復号シード値を生成する。

この構成によると、第１復号検証値を用いて、第２暗号化情報を復号するので、演算が容易である。

ここで、前記共有鍵生成装置は、前記検証値及び前記第１暗号化情報を用いて、前記シード値を暗号化し、前記第２復号手段は、生成された前記第１復号検証値及び受信された前記第１暗号化情報を用いて、前記第２暗号化情報を復号して前記復号シード値を生成する。

この構成によると、第１復号検証値及び第１暗号化情報を用いて、第２暗号化情報を復号するので、不正な第三者は、前記第１復号検証値及び前記第１暗号化情報を知らなければ、シード値を得ることができず、安全性が高まる。

ここで、前記共有鍵生成装置は、前記検証値及び前記第１暗号化情報に一方向性関数を施して関数値を生成し、生成した前記関数値を用いて、前記シード値に暗号化アルゴリズムを施して前記第２暗号化情報を生成し、前記第２復号手段は、前記第１復号検証値及び前記第１暗号化情報に前記一方向性関数を施して復号関数値を生成し、生成した前記復号関数値を用いて、前記第２暗号化情報に、前記暗号化アルゴリズムに対応する復号アルゴリズムを施して、前記復号シード値を生成する。

この構成によると、第２復号手段は、一方向性関数及び復号アルゴリズムの２段階による演算方法を採用しているので、不正な第三者は、第１暗号化情報及び第２暗号化情報を知っていても、少なくとも一方向性関数と復号アルゴリズムとを知らなければ、シード値を得ることができず、安全性が高まる。

ここで、前記共有鍵生成装置は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして排他的論理和を施すことにより、前記第２暗号化情報を生成し、前記第２復号手段は、前記復号関数値及び前記第２暗号化情報に、前記復号アルゴリズムとして、排他的論理和を施すことにより、前記復号シード値を生成する。

この構成によると、前記復号アルゴリズムは、排他的論理和であるので、演算が容易である。また、前記暗号化アルゴリズムの逆演算である。

ここで、前記共有鍵生成装置は、前記シード値に一方向性関数を施して関数値を生成し、生成した前記関数値から前記検証値及び前記共有鍵を生成し、前記共有鍵生成手段は、生成された前記復号シード値に、前記一方向性関数を施して復号関数値を生成し、生成した前記復号関数値から前記第２復号検証値及び前記復号共有鍵を生成する。

この構成によると、前記復号シード値に一方向性関数を施して、前記第２復号検証値を生

成するので、前記第２復号検証値を第三者が知り得たとしても、前記第２復号検証値から前記シード値を求めることは困難である。このため、前記第２復号検証値からシード値を求め、さらに、共有鍵を求めることは事実上不可能である。

ここで、前記共有鍵生成装置は、前記シード値に、前記一方向性関数として、ハッシュ関数を施して前記関数値を生成し、前記共有鍵生成手段は、生成された前記復号シード値に、前記一方向性関数として、前記ハッシュ関数を施して前記復号関数値を生成する。

この構成によると、前記一方向性関数は、ハッシュ関数であるので、その演算アルゴリズムがよく知られており、適用が容易である。

ここで、前記共有鍵生成装置は、生成された前記関数値の一部を前記検証値とし、他の一部を前記共有鍵とすることにより、前記検証値及び前記共有鍵を生成し、前記共有鍵生成手段は、生成された前記復号関数値の一部を前記第２復号検証値とし、他の一部を前記復号共有鍵とすることにより、前記第２復号検証値及び前記復号共有鍵を生成する。

この構成によると、前記復号関数値の一部を前記第２復号検証値とし、他の一部を前記復号共有鍵とするので、前記第２復号検証値及び前記復号共有鍵の生成が容易である。

ここで、前記共有鍵生成装置は、前記シード値に一方向性関数を施して関数値を生成し、生成した前記関数値から前記検証値、前記共有鍵及びブラインド値を生成し、公開鍵を取得し、取得された前記公開鍵及び生成された前記ブラインド値を用いて、前記検証値に公開鍵暗号化アルゴリズムを施して前記第１暗号化情報を生成し、前記共有鍵生成手段は、生成された前記復号シード値に、前記一方向性関数を施して復号関数値を生成し、生成した前記復号関数値から前記第２復号検証値、前記復号共有鍵及び復号ブラインド値を生成する。

この構成によると、前記復号シード値に一方向性関数を施して、前記第２復号検証値を生成するので、前記第２復号検証値を第三者が知り得たとしても、前記第２復号検証値から前記シード値を求めることは困難である。このため、前記第２復号検証値からシード値を求め、さらに、共有鍵を求めることは事実上不可能である。

ここで、前記共有鍵生成装置は、公開鍵を取得し、取得された前記公開鍵及び生成された前記ブラインド値を用いて、前記検証値に公開鍵暗号化アルゴリズムを施して前記第１暗号化情報を生成し、前記判断手段は、前記第１復号検証値及び前記第２復号検証値に基づく前記判断に代えて、前記公開鍵を取得する公開鍵取得部と、取得された前記公開鍵及び生成された前記復号ブラインド値を用いて、生成された前記第１復号検証値又は前記第２復号検証値に前記公開鍵暗号化アルゴリズムを施して再暗号化情報を生成する再暗号化部と、受信された前記第１暗号化情報及び生成された前記再暗号化情報に基づいて、生成された前記復号共有鍵を出力するか否かを判断する判断部とを備える。

この構成によると、受信された前記第１暗号化情報及び生成された前記再暗号化情報に基づいて、生成された前記復号共有鍵を出力するか否かを判断するので、共有鍵生成装置から

第三者に知られることなく共有鍵を受信できると共に、この際に、共有鍵生成装置と共有鍵復元装置との間で異なる共有鍵が導出されるのを防止できるという効果がある。

ここで、前記判断部は、前記第１暗号化情報と前記再暗号化情報とを比較し、前記第１暗号化情報と前記再暗号化情報とが一致する場合に、前記復号共有鍵を出力すると判断する。また、前記判断手段は、前記第１復号検証値と前記第２復号検証値とを比較し、一致する場合に、前記復号共有鍵を出力すると判断する。

この構成によると、第１暗号化情報と再暗号化情報とが一致する場合に、復号共有鍵を出力するので、復号共有鍵を出力するか否かの判断が確実に行える。

ここで、前記公開鍵暗号化アルゴリズムは、ＮＴＲＵ暗号方式によるものであり、前記共有鍵生成装置は、前記公開鍵として、ＮＴＲＵ暗号方式の鍵生成アルゴリズムにより生成された公開鍵多項式を取得し、前記検証値から検証値多項式を生成し、前記ブラインド値からブラインド値多項式を生成し、ＮＴＲＵ暗号方式の暗号化アルゴリズムにより、前記公開鍵多項式を鍵として用い、前記検証値多項式を攪乱するために前記ブラインド値多項式を用いて、前記検証値多項式を暗号化して、多項式としての前記第１暗号化情報を生成し、前記公開鍵取得部は、前記公開鍵多項式を取得し、前記再暗号化部は、前記第２復号検証値から復号検証値多項式を生成し、前記復号ブラインド値から復号ブラインド値多項式を生成し、ＮＴＲＵ暗号方式の暗号化アルゴリズムにより、前記公開鍵多項式を鍵として用い、前記復号検証値多項式を攪乱するために前記復号ブラインド値多項式を用いて、前記復号検証値多項式を暗号化して、多項式としての前記再暗号化情報を生成する。

この構成によると、ＮＴＲＵ暗号を採用することができる。

ここで、前記共有鍵生成装置は、さらに、コンテンツを取得し、生成された前記共有鍵を用いて、取得されたコンテンツを暗号化して、暗号化コンテンツを生成し、生成された前記暗号化コンテンツを送信し、前記受信手段は、さらに、前記暗号化コンテンツを受信し、前記共有鍵復元装置は、さらに、出力された前記復号共有鍵を用いて、受信された前記暗号化コンテンツを復号して、復号コンテンツを生成する復号手段と、生成された復号コンテンツを出力する出力手段とを備える。

この構成によると、共有鍵生成装置は、生成された前記共有鍵を用いて、取得されたコンテンツを暗号化して、暗号化コンテンツを生成し、前記共有鍵復元装置は、出力された前記復号共有鍵を用いて、受信された前記暗号化コンテンツを復号して、復号コンテンツを生成するので、第三者に知られることなく、共有鍵生成装置から共有鍵復元装置へコンテンツを送信することができるという効果がある。

【BRIEF DESCRIPTION OF THE DRAWINGS】

These and the other objects, advantages and features of

the invention will become apparent from the following description thereof taken in conjunction with the accompanying drawings which illustrate a specific embodiment of the invention.

In the drawings:

図１は、コンテンツ配信システム１０の構成と、構成要素の間の接続形態とを示す概念図である。

図２は、暗号装置１１０の構成を示すブロック図である。

図３は、復号装置１２０の構成を示すブロック図である。

図４は、暗号装置１１０及び復号装置１２０の動作を示す処理系統図である。

図５は、暗号装置１１０及び復号装置１２０の動作を示すフローチャートである。

図６は、暗号装置１１０ｂの構成を示すブロック図である。

図７は、復号装置１２０ｂの構成を示すブロック図である。

図８は、暗号装置１１０ｂ及び復号装置１２０ｂの動作を示す処理系統図である。

図９は、暗号装置１１０ｃの構成を示すブロック図である。

図１０は、復号装置１２０ｃの構成を示すブロック図である。

図１１は、暗号装置１１０ｃ及び復号装置１２０ｃの動作を示す処理系統図である。

図１２は、暗号装置１１０ｃ及び復号装置１２０ｃの変形例の動作を示す処理系統図である。

図１３は、暗号装置１１０ｄの構成を示すブロック図である。

図１４は、復号装置１２０ｄの構成を示すブロック図である。

図１５は、暗号装置１１０ｄ及び復号装置１２０ｄの動作を示すフローチャートである。

図１６は、暗号装置１１０ｄ及び復号装置１２０ｄの動作を示す処理系統図である。

図１７は、暗号装置１１０ｅの構成を示すブロック図である。

図１８は、復号装置１２０ｅの構成を示すブロック図である。

図１９は、暗号装置１１０ｅ及び復号装置１２０ｅの動作を示す処理系統図である。

図２０は、暗号装置１１０ｅ及び復号装置１２０ｅの変形例の動作を示す処理系統図である。

【DESCRIPTION OF THE PREFERRED EMBODIMENT】

１．実施の形態１

本発明に係る１個の実施の形態としてのコンテンツ配信システム１０について説明する。コンテンツ配信システム１０は、ＮＴＲＵ暗号を用いて鍵カプセル化メカニズムによる鍵配送を行って暗号化通信を行う暗号通信システムである。

１．１　ＮＴＲＵ暗号方式

コンテンツ配信システム１０において用いるＮＴＲＵ暗号方式について簡単に説明する。ＮＴＲＵ暗号方式は、多項式の演算を用いて暗号化と復号化とを行う公開鍵暗号方式である。

なお、ＮＴＲＵ暗号方式及びＮＴＲＵ暗号方式における公開鍵と秘密鍵との生成方法については、非特許文献２に詳しく述べられている。

（１）ＮＴＲＵ暗号方式のシステムパラメータ

ＮＴＲＵ暗号方式においては、整数のシステムパラメータ、Ｎ、ｐ、ｑが存在し、後述する暗号装置及び復号装置は、これらのシステムパラメータを有している。

上記文献には、システムパラメータの例として、（Ｎ，ｐ，ｑ）＝（１０７，３，６４）、（Ｎ，ｐ，ｑ）＝（１６７，３，１２８）、（Ｎ，ｐ，ｑ）＝（５０３，３，２５６）の３つの例が挙げられている。

以降、本実施の形態では、システムパラメータＮ＝１６７として、説明を行う。

（２）ＮＴＲＵ暗号方式の多項式演算

ＮＴＲＵ暗号方式は、上述したように、多項式の演算により暗号化と復号化を行う公開鍵暗号方式である。

ＮＴＲＵ暗号方式で扱う多項式は、上記システムパラメータＮに対し、Ｎ－１次元以下の多項式である。例えば、Ｎ＝５のとき、Ｘ＾４＋Ｘ＾３＋１等の多項式である。ここで、「Ｘ＾ａ」はＸのａ乗を意味することとする。

また、暗号化時又は復号化時に用いる公開鍵ｈ、秘密鍵ｆ、平文ｍ、乱数ｒ、暗号文ｃはいずれも、Ｎ－１次元以下の多項式として表現される（以降、それぞれを公開鍵多項式ｈ、秘密鍵多項式ｆ、平文多項式ｍ、乱数多項式ｒ、暗号文多項式ｃと呼ぶ）。

多項式演算において、上記システムパラメータＮに対し、関係式Ｘ＾Ｎ＝１を用いて、演算結果が常にＮ－１次元以下の多項式になるように演算される。

例えば、Ｎ＝５の場合、多項式Ｘ＾４＋Ｘ＾２＋１と多項式Ｘ＾３＋Ｘの積は、多項式と多項式の積を×、整数と多項式の積を・とすると、Ｘ＾５＝１という関係から、

（Ｘ＾４＋Ｘ＾２＋１）×（Ｘ＾３＋Ｘ）
＝Ｘ＾７＋２・Ｘ＾５＋２・Ｘ＾３＋Ｘ
＝Ｘ＾２×１＋２・１＋２・Ｘ＾３＋Ｘ
＝２・Ｘ＾３＋Ｘ＾２＋Ｘ＋２

となる。

このように、多項式演算において、常にＮ－１次元以下の多項式になるように演算される。

（３）ＮＴＲＵ暗号方式の暗号化

後述する暗号装置は、次に示すようにＮＴＲＵ暗号方式の暗号化を行う。

暗号化時には、以下に述べる乱数多項式ｒと公開鍵多項式ｈとを用いて、平文多項式ｍに多項式演算である暗号化アルゴリズムＥを施して、

暗号文多項式ｃ＝Ｅ（ｍ，ｒ，ｈ）を生成する。

ここで、Ｅ（ｍ，ｒ，ｈ）は、ＮＴＲＵ暗号方式の暗号化アルゴリズムＥに、平文多項式ｍ、乱数多項式ｒ及び公開鍵多項式ｈを入力して得られる多項式演算の結果である。暗号化アルゴリズムＥについては非特許文献２に詳しく述べられており、ここでは説明を省略する。

なお、ＮＴＲＵ暗号方式では、乱数多項式ｒを生成するためのパラメータｄが予め決められている。乱数多項式ｒは、乱数多項式ｒを構成する各項のうち、ｄ個の項についてはその係数が「１」となり、他のｄ個の項については係数が「－１」となり、残りの項については係数は「０」となるように、選ばれる。

すなわち、乱数多項式ｒは、Ｎ－１次元以下の多項式であり、０次元（定数項）からＮ－１次元までのＮ項について、Ｎ個の係数が存在する。乱数多項式ｒは、このＮ個の係数のうち、ｄ個の係数が「１」であり、かつｄ個の係数が「－１」であり、かつ（Ｎ－２ｄ）個の係数は「０」となるように、選ばれる。

非特許文献２によれば、パラメータＮ＝１６７の場合、ｄ＝１８である。すなわち、１８個の係数が「１」であり、かつ１８個の係数が「－１」であり、１３１（＝１６７－３６）個の係数が「０」となるように、乱数多項式ｒが選ばれる。

（４）ＮＴＲＵ暗号方式の復号化

後述する復号装置は、次に示すようにＮＴＲＵ暗号方式の復号化を行う。

復号化時には、秘密鍵多項式ｆを用いて、暗号文多項式ｃに多項式演算である復号アルゴリズムＤを施して、復号文多項式m'＝Ｄ（ｃ，ｆ）を生成する。

ここで、Ｄ（ｃ，ｆ）は、ＮＴＲＵ暗号方式の復号アルゴリズムＤに、暗号文多項式ｃ、及び秘密鍵多項式ｆを入力して得られる多項式演算の結果である。復号アルゴリズムＤについては非特許文献２に詳しく述べられており、ここでは説明を省略する。

（５）ＮＴＲＵ暗号方式の復号エラー

ところで、このＮＴＲＵ暗号方式において、生成された復号文多項式m'が平文多項式ｍと異なる場合が発生する。この場合は、復号時に正しく平文多項式ｍが得られないことになる。このことを復号エラーが発生するという。

１．２　コンテンツ配信システム１０の構成

コンテンツ配信システム１０は、図１に示すように、コンテンツサーバ装置１４０と暗号装置１１０と復号装置１２０と再生装置１５０とモニタ１５５とから構成されており、コンテンツサーバ装置１４０と暗号装置１１０とは、専用回線２０を介して接続されており、暗号装置１１０と復号装置１２０とは、インターネット１３０を介して接続されている。再生装置１５０は、復号装置１２０及びスピーカを内蔵するモニタ１５５に接続されている。暗号装置１１０には、メモリカード１６０が装着され、復号装置１２０には、メモリカード１７０が装着される。

コンテンツサーバ装置１４０は、映像と音声から構成される映画などのコンテンツを専用回線２０を介して暗号装置１１０へ送信する。

暗号装置１１０と復号装置１２０とは、それぞれ同一の共有鍵K及び共有鍵K'を生成する。次に、暗号装置１１０は、コンテンツサーバ装置１４０から受け取ったコンテンツを共有鍵Kを用いて暗号化して暗号化コンテンツを生成し、生成した暗号化コンテンツを送信し、復号装置１２０は、暗号化コンテンツを受信し、受信した暗号化コンテンツを復号して再生コンテンツを生成し、再生装置１５０は、再生コンテンツから映像信号及び音声信号を生成し、モニタ１５５は、映像を表示し、音声を出力する。

１．３　コンテンツサーバ装置１４０の構成

コンテンツサーバ装置１４０は、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレィユニット、通信ユニット、キーボード、マウスなどから構成されるコンピュータシステムである（図示していない）。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、コンテンツサーバ装置１４０は、その一部の機能を達成する。

コンテンツサーバ装置１４０は、前記コンテンツを予め記憶しており、前記コンテンツは、複数の部分コンテンツmi（$1 \leqq i \leqq n$）から構成されている。コンテンツサーバ装置１４０は、暗号装置１１０の要求に応じて、部分コンテンツmiを読み出し、読み出した部分コンテンツmiを、専用回線２０を介して暗号装置１１０へ送信する。

１．４　メモリカード１６０及びメモリカード１７０の構成

メモリカード１６０は、記憶媒体としてフラッシュメモリを採用しているカード型の記憶装置であり、予め公開鍵多項式hを記憶している。

また、メモリカード１７０は、メモリカード１６０と同様のカード型の記憶装置であり、予め秘密鍵多項式f及び公開鍵多項式hを記憶している。

ここで、秘密鍵多項式fと公開鍵多項式hとは、NTRU暗号方式により生成されたものであり、それぞれ対応している。

１．５　暗号装置１１０の構成

暗号装置１１０は、図２に示すように、公開鍵入力部１１１、乱数生成部１１２、第１関数部１１３、暗号化部１１４、第１送信部１１７、共通鍵暗号部１１８及び第２送信部１１９から構成されている。

暗号装置１１０は、具体的には、マイクロプロセッサ、ROM、RAM、通信ユニットなどから構成されるコンピュータシステムである。前記RAMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作

することにより、暗号装置１１０は、その機能を達成する。

（1）公開鍵入力部１１１

公開鍵入力部１１１は、メモリカード１６０から復号装置１２０の公開鍵多項式ｈを読み出し、読み出した公開鍵多項式ｈを暗号化部１１４へ出力する。

（2）乱数生成部１１２

乱数生成部１１２は、共有鍵Ｋを生成するための元となるシード値として、乱数ｓを生成し、生成した乱数ｓを第１関数部１１３と暗号化部１１４とへ出力する。

（3）第１関数部１１３

第１関数部１１３は、乱数生成部１１２から乱数ｓを受け取り、乱数ｓの関数値Ｇ（ｓ）を生成する。ここで、関数Ｇは、出力長が２ｋビットのハッシュ関数である。なお、ハッシュ関数は、一方向性関数の一種である。次に、第１関数部１１３は、関数値Ｇ（ｓ）の上位ｋビットを乱数値ｕとし、Ｇ（ｓ）の下位ｋビットを共有鍵Ｋとすることにより、生成した関数値Ｇ（ｓ）から共有鍵Ｋと乱数値ｕとを生成し、生成した乱数値ｕを暗号化部１１４へ出力し、生成した共有鍵Ｋを共通鍵暗号部１１８へ出力する。

（4）暗号化部１１４

暗号化部１１４は、公開鍵入力部１１１から公開鍵多項式ｈを受け取り、乱数生成部１１２から乱数ｓを受け取り、第１関数部１１３から乱数値ｕを受け取る。次に、以下のようにして、ＮＴＲＵ暗号により、公開鍵多項式ｈと乱数値ｕとを用いて乱数ｓの第１暗号文ｃ１を生成する。ここで、乱数値ｕは、ブラインド値であり、暗号化の対象である乱数ｓを不明瞭にするために用いられる。

暗号化部１１４は、ＮＴＲＵ暗号のパラメータｄに対し、乱数多項式ｒのｄ個の項の係数が「１」であり、ｄ個の項の係数が「－１」であり、残りの項の係数が「０」である乱数多項式ｒを乱数値ｕから一意に求まるように生成する。

例えば、暗号化部１１４は、乱数値ｕを擬似乱数系列の初期値（乱数シード）として設定し、{0，1，...，Ｎ－1} から重複しないように２ｄ個の擬似乱数を生成し、最初のｄ個の疑似乱数によりそれぞれ示されるｄ個の次元の項の係数を「１」とし、残りのｄ個の擬似乱数によりそれぞれ示されるｄ個の次元の項の係数を「－１」とし、他の次元の項の係数は「０」とする。

次に、暗号化部１１４は、乱数ｓがＮＴＲＵ暗号の暗号アルゴリズムＥに適用できるように、乱数ｓを２進数表現した場合のＮ桁のビット列の各桁の値が、乱数多項式ｓｐの各項の係数に対応するように、乱数多項式ｓｐを構成する。例えば、乱数ｓの下位ｂビット目の値を、項Ｘ＾ｂの係数とする。具体的には、ｓ＝１００１０（ビット表現）の場合、乱数多項式ｓｐ＝Ｘ＾５＋Ｘ＾２を生成する。

次に、暗号化部１１４は、公開鍵多項式ｈを使用して、乱数多項式ｒを用いて乱数多項式

ｓｐに前記暗号アルゴリズムＥを施して、

第１暗号文ｃ１＝暗号文多項式Ｅ（ｓｐ，ｒ，ｈ）を生成する。

次に、暗号化部１１４は、生成した第１暗号文ｃ１を第１送信部１１７へ出力する。

なお、図２において、暗号装置１１０の各構成部を示す各ブロックは、接続線により他のブロックと接続されている。ここで、各接続線は、信号や情報が伝達される経路を示している。また、暗号化部１１４を示すブロックに接続している複数の接続線のうち、接続線上に鍵マークが付されているものは、暗号化部１１４へ鍵としての情報が伝達される経路を示している。共通鍵暗号部１１８を示すブロックについても同様である。また、他の図面についても同様である。

（５）第１送信部１１７

第１送信部１１７は、暗号化部１１４から第１暗号文ｃ１を受け取り、第１暗号文ｃ１をインターネット１３０を介して復号装置１２０へ送信する。

（６）共通鍵暗号部１１８

共通鍵暗号部１１８は、例えばＤＥＳ暗号方式のような共通鍵暗号アルゴリズムＳｙｍを有している。

一般的に、共通鍵暗号では、暗号側の装置において、暗号鍵Ｋを用いて、平文ｍに共通鍵暗号アルゴリズムＳｙｍを施して、暗号文ｃ＝Ｓｙｍ（ｍ，Ｋ）を生成し、復号側の装置において、暗号鍵Ｋを用いて、暗号文ｃに共通鍵暗号アルゴリズムＳｙｍを施して、復号文ｍ'＝Ｓｙｍ（ｃ，Ｋ）を生成する。ここで、暗号文生成時に用いる暗号鍵Ｋと復号文生成時に用いる暗号鍵Ｋが同一であれば、ｍ'＝ｍとなる。なお、共通鍵暗号及びＤＥＳ暗号方式については、非特許文献１に詳しく述べられているため、ここでの詳細な説明は省略する。

共通鍵暗号部１１８は、コンテンツサーバ装置１４０から複数の平文（部分コンテンツ）ｍｉ（１≦ｉ≦ｎ）を受け取り、第１関数部１１３から共有鍵Ｋを受け取り、受け取った共有鍵Ｋを使用して平文ｍｉ（１≦ｉ≦ｎ）に共通鍵暗号アルゴリズムＳｙｍを施して、共通鍵暗号文Ｃｉ＝Ｓｙｍ（ｍｉ，Ｋ）（１≦ｉ≦ｎ）を生成する。

次に、共通鍵暗号部１１８は、共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を第２送信部１１９へ出力する。

（７）第２送信部１１９

第２送信部１１９は、共通鍵暗号部１１８から共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を受け取り、受け取った共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を、インターネット１３０を介して復号装置１２０へ送信する。

１．６　復号装置１２０の構成

復号装置１２０は、図３に示すように、秘密鍵入力部１２１、第１受信部１２２、復号化部１２３、第２関数部１２６、比較部１２７、共通鍵復号部１２８及び第２受信部１２９か

ら構成される。

復号装置１２０は、暗号装置１１０と同様のコンピュータシステムである。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、復号装置１２０は、その機能を達成する。

（1）秘密鍵入力部１２１

秘密鍵入力部１２１は、メモリカード１７０から、復号装置１２０の秘密鍵多項式ｆと公開鍵多項式ｈとを読み出し、読み出した秘密鍵多項式ｆを復号化部１２３へ出力し、読み出した公開鍵多項式ｈを比較部１２７へ出力する。

（2）第１受信部１２２

第１受信部１２２は、インターネット１３０を介して暗号装置１１０から第１暗号文ｃ１を受け取り、受け取った第１暗号文ｃ１を復号化部１２３へ出力する。

（3）復号化部１２３

復号化部１２３は、秘密鍵入力部１２１から秘密鍵多項式ｆを受け取り、第１受信部１２２から第１暗号文ｃ１を受け取り、次に示すようにして、ＮＴＲＵ暗号により、秘密鍵多項式ｆを用いて、第１暗号文ｃ１を復号して復号乱数ｓ’を生成する。

復号化部１２３は、秘密鍵多項式ｆを使用して、第１暗号文ｃ１に前記復号アルゴリズムＤを施して、復号乱数多項式ｓｐ’＝Ｄ（ｃ１，ｆ）を生成する。次に、復号乱数多項式ｓｐ’は、ＮＴＲＵ暗号の復号文であり多項式で表現されているので、復号乱数多項式ｓｐ’の各項の係数が、復号乱数ｓ’を２進数表現した場合のＮ桁のビット列の各値に対応するように、復号乱数ｓ’を生成する。例えば、復号乱数多項式ｓｐ’のｂ次元の項Ｘ＾ｂの係数は、復号乱数ｓ’の下位ｂビット目の値となる。

具体的には、復号乱数多項式ｓｐ’＝Ｘ＾５＋Ｘ＾２の場合、復号乱数ｓ’＝１００１０（ビット表現）を生成する。

次に、復号化部１２３は、受け取った第１暗号文ｃ１と生成した復号乱数ｓ’とを比較部１２７へ出力し、生成した復号乱数ｓ’を第２関数部１２６へ出力する。

（4）第２関数部１２６

第２関数部１２６は、第１関数部１１３が有している関数と同じ関数Ｇのアルゴリズムを有している。

第２関数部１２６は、復号化部１２３から復号乱数ｓ’を受け取り、第１関数部１１３と同様にして、復号乱数ｓ’の関数値Ｇ（ｓ’）を生成し、次に、関数値Ｇ（ｓ’）から乱数値ｕ’と共有鍵Ｋ’とを生成し、生成した乱数値ｕ’と共有鍵Ｋ’とを比較部１２７へ出力する。

（5）比較部１２７

比較部１２７は、図３に示すように、暗号化部１２７ｘと比較演算部１２７ｙとから構成

されている。

暗号化部１２７ｘは、秘密鍵入力部１２１から公開鍵多項式ｈを受け取り、復号化部１２３から復号乱数ｓ’を受け取り、第２関数部１２６から乱数値ｕ’を受け取る。次に、暗号化部１１４と同様にして、公開鍵多項式ｈと乱数値ｕ’とを用いて、復号乱数ｓ’を暗号化して第１再暗号文ｃ１’を生成し、生成した第１再暗号文ｃ１’を比較演算部１２７ｙへ出力する。

比較演算部１２７ｙは、復号化部１２３から第１暗号文ｃ１を受け取り、第２関数部１２６から共有鍵K’を受け取り、暗号化部１２７ｘから第１再暗号文ｃ１’を受け取る。次に、第１暗号文ｃ１と第１再暗号文ｃ１’とを比較して、一致しているか否かを判断し、一致していると判断する場合に、受け取った共有鍵K’を共通鍵復号部１２８へ出力する。一致しないと判断する場合に、受け取った共有鍵K’を出力しない。

（６）第２受信部１２９

第２受信部１２９は、インターネット１３０を介して暗号装置１１０から共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を受信し、受信した共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を共通鍵復号部１２８へ出力する。

（７）共通鍵復号部１２８

共通鍵復号部１２８は、共通鍵暗号部１１８が有する共通鍵暗号アルゴリズムＳｙｍと同じ共通鍵暗号アルゴリズムＳｙｍを予め有している。

共通鍵復号部１２８は、比較部１２７から共有鍵K’を受け取り、第２受信部１２９から共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を受け取り、受け取った共有鍵K’を使用して受け取った共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）に共通鍵暗号アルゴリズムＳｙｍを施して、復号文ｍｉ’＝Ｓｙｍ（Ｃｉ，Ｋ）（１≦ｉ≦ｎ）を生成する。

次に、共通鍵復号部１２８は、生成した復号文ｍｉ’（１≦ｉ≦ｎ）を再生装置１５０へ出力する。

１．７　再生装置１５０及びモニタ１５５

再生装置１５０は、復号装置１２０から復号文ｍｉ’（１≦ｉ≦ｎ）を受け取り、受け取った復号文ｍｉ’（１≦ｉ≦ｎ）から映像信号及び音声信号を生成し、生成した映像信号及び音声信号をモニタ１５５へ出力する。

モニタ１５５は、再生装置１５０から映像信号及び音声信号を受け取り、受け取った映像信号及び音声信号により、映像を表示し、音声を出力する。

１．８　暗号装置１１０及び復号装置１２０の動作

暗号装置１１０及び復号装置１２０の動作について、図４に示す処理系統図及び図５に示すフローチャートを用いて説明する。

暗号装置１１０の公開鍵入力部１１１は、メモリカード１６０から復号装置１２０の公開

鍵多項式ｈを読み出し、読み出した公開鍵多項式ｈを暗号化部１１４へ出力する（ステップＳ１０１）。

次に、乱数生成部１１２は、乱数ｓを生成し、生成した乱数ｓを第１関数部１１３と暗号化部１１４とへ出力する（ステップＳ１０２）。

次に、第１関数部１１３は、乱数生成部１１２から乱数ｓを受け取り、乱数ｓの関数値Ｇ（ｓ）を生成し（ステップＳ１０３）、次に、第１関数部１１３は、関数値Ｇ（ｓ）から乱数値ｕと共有鍵Ｋとを生成して、乱数値ｕを暗号化部１１４へ出力し、共有鍵Ｋを共通鍵暗号部１１８へ出力する（ステップＳ１０４）。

次に、暗号化部１１４は、公開鍵入力部１１１から公開鍵多項式ｈを受け取り、乱数生成部１１２から乱数ｓを受け取り、第１関数部１１３から乱数値ｕを受け取り、公開鍵多項式ｈと乱数値ｕを用いて乱数ｓの第１暗号文ｃ１を生成し、第１暗号文ｃ１を第１送信部１１７へ出力する（ステップＳ１０５）。

次に、第１送信部１１７は、暗号化部１１４から第１暗号文ｃ１を受け取り、第１暗号文ｃ１をインターネット１３０を介して復号装置１２０へ送信する（ステップＳ１０６）。

次に、復号装置１２０の秘密鍵入力部１２１は、メモリカード１７０から復号装置１２０の秘密鍵多項式ｆと公開鍵多項式ｈとを読み出し、読み出した秘密鍵多項式ｆを復号化部１２３へ出力し、読み出した公開鍵多項式ｈを比較部１２７へ出力する（ステップＳ１５１）。

次に、第１受信部１２２は、インターネット１３０を介して暗号装置１１０から第１暗号文ｃ１を受け取り、第１暗号文ｃ１を復号化部１２３へ出力する（ステップＳ１０６）。

次に、復号化部１２３は、秘密鍵入力部１２１から秘密鍵多項式ｆを受け取り、第１受信部１２２から第１暗号文ｃ１を受け取り、次に、秘密鍵多項式ｆを用いて、第１暗号文ｃ１を復号して復号乱数ｓ’を生成し、第１暗号文ｃ１と復号乱数ｓ’を比較部１２７へ出力し、復号乱数ｓ’を第２関数部１２６へ出力する（ステップＳ１５２）。

次に、第２関数部１２６は、復号化部１２３から復号乱数ｓ’を受け取り、復号乱数ｓ’の関数値Ｇ（ｓ’）を生成し（ステップＳ１５３）、関数値Ｇ（ｓ’）から乱数値ｕ’と共有鍵Ｋ’とを生成して、乱数値ｕ’と共有鍵Ｋ’とを比較部１２７へ出力する（ステップＳ１５４）。

次に、比較部１２７は、復号化部１２３から第１暗号文ｃ１を受け取り、第２関数部１２６から乱数値ｕ’と共有鍵Ｋ’とを受け取り、第１再暗号文ｃ１’を生成し（ステップＳ１５５）、第１暗号文ｃ１が乱数値ｕ’を用いた復号乱数ｓ’の暗号文であるかどうかチェックを行い、第１暗号文ｃ１が復号乱数ｓ’の暗号文でなければ（ステップＳ１５６）、復号装置１２０は、処理を終了する。

共通鍵暗号部１１８は、外部から複数の平文ｍｉ（１≦ｉ≦ｎ）を受け取り、第１関数部１１３から共有鍵Ｋを受け取り、共有鍵Ｋを使用して平文ｍｉ（１≦ｉ≦ｎ）に共通鍵暗号

アルゴリズムＳｙｍを施して、共通鍵暗号文Ｃｉ＝Ｓｙｍ（ｍｉ，Ｋ）（１≦ｉ≦ｎ）を生成し、共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を第２送信部１１９へ出力する（ステップＳ１０７）。

次に、第２送信部１１９は、共通鍵暗号部１１８から共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を受け取り、インターネット１３０を介して復号装置１２０へ送信し（ステップＳ１０８）、処理を終了する。

第１暗号文ｃ１が復号乱数ｓ’の暗号文であれば（ステップＳ１５６）、比較部１２７は、共有鍵Ｋ’を共通鍵復号部１２８へ出力する（ステップＳ１５７）。次に、第２受信部１２９は、インターネット１３０を介して暗号装置１１０から暗号文Ｃｉ（１≦ｉ≦ｎ）を受信し、共通鍵復号部１２８へ出力する（ステップＳ１０８）。

次に、共通鍵復号部１２８は、比較部１２７から共有鍵Ｋ’を受け取り、第２受信部１２９から共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を受け取り、共有鍵Ｋ’を使用して共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）に共通鍵暗号アルゴリズムＳｙｍを施して、復号文ｍｉ’＝Ｓｙｍ（Ｃｉ，Ｋ）（１≦ｉ≦ｎ）を生成し、復号文ｍｉ’（１≦ｉ≦ｎ）を再生装置１５０へ出力し（ステップＳ１５８）、処理を終了する。

１．９　コンテンツ配信システム１０の動作検証

以下に、実施の形態１におけるコンテンツ配信システム１０の全体の動作について説明する。

まず、暗号装置１１０は、復号装置１２０の公開鍵多項式ｈを入力とし、乱数ｓを生成し、関数値Ｇ（ｓ）から乱数値ｕと共有鍵Ｋとを導出する。次に、暗号装置１１０は、乱数ｓを、公開鍵多項式ｈと乱数値ｕを用いてＮＴＲＵ暗号で暗号化して第１暗号文ｃ１を生成し、第１暗号文ｃ１をインターネット１３０を介して復号装置１２０へ送信する。

すなわち、この暗号装置１１０は、以下の処理を行い、第１暗号文ｃ１を復号装置１２０へ送信する。

・乱数ｓを生成する。

・Ｇ（ｓ）を生成し、Ｇ（ｓ）からｕ、Ｋを生成する。

・公開鍵多項式ｈと乱数値ｕとを用いて乱数ｓの第１暗号文ｃ１を生成する。

・共有鍵Ｋと第１暗号文ｃ１とを出力する。

次に、暗号装置１１０は、導出した共有鍵Ｋを用いて、外部から入力された平文ｍｉ（１≦ｉ≦ｎ）を共通鍵暗号で暗号化して暗号文Ｃｉ（１≦ｉ≦ｎ）を生成し、インターネット１３０を介して復号装置１２０へ送信する。

一方、復号装置１２０は、復号装置１２０の秘密鍵多項式ｆ及び公開鍵多項式ｈを入力とし、インターネット１３０を介して暗号装置１１０から第１暗号文ｃ１を受信し、第１暗号文ｃ１を秘密鍵多項式ｆを用いて復号して復号乱数ｓ’を生成する。次に、復号乱数ｓ’の関数値Ｇ（ｓ’）から乱数値ｕ’と共有鍵Ｋ’を導出し、復号乱数ｓ’を暗号化して第１再暗

号文ｃ１’を生成し、ｃ１’＝ｃ１であれば、共有鍵K’を出力する。

すなわち、この復号装置１２０は、以下の処理を行い、共有鍵K’を導出する。

・秘密鍵多項式ｆを用いて第１暗号文ｃ１を復号してｓ’を生成する。

・Ｇ（ｓ’）を生成し、Ｇ（ｓ’）からｕ’、K’を生成する。

・公開鍵多項式ｈ、乱数値ｕ’を用いてｓ’の第１再暗号文ｃ１’を生成する。

・ｃ１’＝ｃ１が成立するかどうかチェックする。成立すれば共有鍵K’を出力する。

ここで、暗号装置１１０で用いられた公開鍵多項式ｈに対応する正しい秘密鍵多項式ｆが復号装置１２０で用いられれば、第１暗号文ｃ１は正しく復号されて、復号乱数ｓ’＝ｓとなり、従って、Ｇ（ｓ’）から導出される乱数値ｕ’＝ｕとなり、共有鍵K’＝Kとなる。そして、ｓ’＝ｓ及びｕ’＝ｕが成り立つので、ｃ１’＝ｃ１が成り立ち、復号装置１２０は暗号装置１１０と同じ共有鍵Kを導出できることになる。

次に、復号装置１２０は、導出した共有鍵K’（＝K）を用いて、インターネットを介して暗号装置１１０から共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を共通鍵暗号で復号して復号文ｍｉ’（１≦ｉ≦ｎ）を生成して外部へ出力する。ここで、共通鍵暗号文生成時に用いた暗号鍵Kと復号文生成時に用いる暗号鍵K’とは同一であるで、復号装置１２０は、正しくｍｉ'＝ｍｉ（１≦ｉ≦ｎ）を得ることができる。

なお、復号エラーが発生した場合には、復号乱数ｓ’と乱数ｓとは異なるので、Ｇ（ｓ’）から導出される乱数値ｕ’及び共有鍵K’は、それぞれｕ、Kとは異なる。しかし、この場合、ｓ’、ｕ’がそれぞれｓ、ｕと異なるために第１再暗号文ｃ１’が第１暗号文ｃ１と異なるので、復号装置１２０は、共有鍵K’を出力しない。

１．１０　実施の形態１における効果

従来のＲＳＡ－ＫＥＭアルゴリズムでは、秘密鍵を知らなければ暗号文Ｃから導出できない要素ｓをハッシュ関数Ｇに入力して共有鍵Kを導出する。しかしながら、ＮＴＲＵ暗号を用いて、鍵カプセル化メカニズムであるＲＳＡ－ＫＥＭアルゴリズムを適用して共有鍵の配送を行おうとすると、復号エラーが発生する場合があるため、秘密鍵を用いても要素ｓが導出できず、従って正しくない共有鍵K’を導出する場合がある。

しかしながら、実施の形態１のコンテンツ配信システム、暗号装置及び復号装置においては、乱数ｓのハッシュ関数値Ｇ（ｓ）から共有鍵に加えて乱数値ｕを生成し、復号装置が乱数値ｕと公開鍵多項式ｈとを用いて復号乱数ｓ’を再暗号化して第１再暗号文ｃ１’を生成し、第１再暗号文ｃ１’が第１暗号文ｃ１と同じ値でない限り共有鍵K’を出力しないようにしたので、復号エラーが発生した場合、暗号装置と復号装置との間で異なる鍵が導出されるのを防止できる。

また、本発明による方式は、非特許文献３に記述されている証明方法と同様の方法により、理論的にその安全性が証明できる。

１．１１　変形例

上記に説明した実施の形態１は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その主旨を逸脱しない範囲において種々なる態様で実施し得るものである。以下のような場合も本発明に含まれる。

（１）用いるＮＴＲＵ暗号のパラメータＮ＝１６７に限定されない。パラメータＮは、他の値をとるとしてもよい。

（２）暗号化部１１４及び復号化部１２３で行われるビット列の各ビットの値と多項式の各項の係数との変換方法は、上記において説明した方法に限られず他の変換方法でもよい。

例えば、乱数ｓから乱数多項式ｓｐへの変換は、ビット列の各ビットの値と多項式の各項の係数とを１対１に対応させる関数を用いて変換してもよいし、また、ビット列の各ビットの値と多項式の各項の係数とを１対１に対応させて記憶している関数値テーブルを用いて変換してもよい。

また、乱数値ｕから乱数多項式ｒへの変換は、ｕからｒが一意に求まり、ｒのｄ個の次元の項の係数を「１」とし、ｄ個の次元の項の係数を「－１」とし、他の次元の項の係数は「０」となるようにすれば、他の変換方法でもよく、例えば、乱数値ｕを多項式に対応させる関数、又は関数値テーブルを用いて変換してもよい。

（３）暗号化部１１４及び復号化部１２３で用いる公開鍵暗号方式は、暗号化部１１４において、乱数ｓを公開鍵と乱数値ｕを用いて暗号化して第１暗号文ｃ１を生成し、復号化部１２３において、第１暗号文ｃ１を秘密鍵で復号して乱数値ｓと等しい復号乱数ｓ’を生成できるものであればよい。

従って、暗号化部１１４及び復号化部１２３で用いる公開鍵暗号は、ＮＴＲＵ暗号以外に、どんな公開鍵暗号でも利用できる。

例えば、ＥｌＧａｍａｌ暗号を採用するならば、ｈ、ｆをそれぞれＥｌＧａｍａｌ暗号の公開鍵、秘密鍵とし、暗号化部１１４において、乱数ｓをｈとｕを用いて暗号化してｃ１を生成し、復号化部１２３において、ｃ１をｆを用いて復号してｓ’を生成すればよい。

なお、ＥｌＧａｍａｌ暗号について非特許文献１に詳細に記載されているため、ここでは説明を省略する。

（４）第１関数部１１３は、関数値Ｇ（ｓ）の上位ｋビットを乱数値ｕとし、下位ｋビットを共有鍵Ｋとする以外に、関数値Ｇ（ｓ）から乱数値ｕと共有鍵Ｋとを導出すれば他の方法でもよい。

例えば、関数値Ｇ（ｓ）の上位ｋ／２ビットを乱数値ｕとし、下位ｋ×３／２ビットを共有鍵Ｋとしてもよい。また、関数値Ｇ（ｓ）の２ｋビットのうち、１ビット置きにｋビットを選択して乱数値ｕとし、残りのｋビットを共有鍵Ｋとしてもよい。

（５）乱数値ｕは、第１関数部１１３及び第２関数部１２６で生成される以外にも、暗号

装置１１０と復号装置１２０とで同じ値を得られれば、他の生成方法を採用してもよい。

例えば、任意の関数Ｆｕｎｃに対し、ｕ＝Ｆｕｎｃ（ｓ）として暗号装置１１０と復号装置１２０とで同じ値を得られるようにしてもよい。すなわち、暗号装置１１０と復号装置１２０とにおいて、

・Ｇ（ｓ）を生成し、Ｇ（ｓ）からＫを生成する。

・Ｆｕｎｃ（ｓ）を生成し、ｕ＝Ｆｕｎｃ（ｓ）とする。

としてもよい。

（６）乱数値ｕは、第１関数部１１３及び第２関数部１２６で生成される以外にも、暗号装置１１０と復号装置１２０とで同じ値を得られればよいので、暗号装置１１０が乱数値ｕを復号装置１２０ｂに直接送信してもよい。

すなわち、以下のように、第１暗号文ｃ１と乱数値ｕを復号装置１２０に送信してもよい。このとき、乱数値ｕは暗号化して送信されてもよい。

暗号装置１１０において、

・Ｇ（ｓ）を生成し、Ｇ（ｓ）からＫを生成する。

・乱数値ｕを、別途、暗号装置１１０から復号装置１２０へ送信する。

復号装置１２０において、

・乱数値ｕを受信する。

・乱数値ｕ’に代えて、受信した乱数値ｕを用いて第１再暗号文ｃ１’を生成する。

このとき、暗号装置１１０は、乱数値ｕを暗号化して送信し、復号装置１２０は、暗号化された乱数値ｕを復号するとしてもよい。

（７）乱数値ｕは、暗号装置１１０と復号装置１２０とで同じ値を得られればよいので、乱数値ｕの一部分の部分情報を第１関数部１１３及び第２関数部１２６で生成し、乱数値ｕの残りの部分の部分情報を暗号装置１１０から復号装置１２０に直接送信してもよい。

例えば、以下のように、暗号装置１１０は、第１暗号文ｃ１と乱数値ｕ２とを復号装置１２０に送信してもよい。

暗号装置１１０において、

（ａ）Ｇ（ｓ）を生成し、Ｇ（ｓ）からＫ、ｕ１を生成する。

（ｂ）乱数値ｕ２を生成し、別途、復号装置１２０へ送信する。

（ｃ）乱数値ｕを、ｕ＝ｕ１　ｘｏｒ　ｕ２から生成する。

（ｄ）乱数値ｕを用いて、第１暗号文ｃ１を生成する。

復号装置１２０において、

（ｅ）乱数値ｕ２を受信する。

（ｆ）Ｇ（ｓ’）を生成し、Ｇ（ｓ’）からＫ’、ｕ１’を生成する。

（ｇ）乱数値ｕ’を、ｕ’＝ｕ１’　ｘｏｒ　ｕ２から生成する。

（h）生成した乱数値u'を用いて第1再暗号文c1'を生成する。

このとき、暗号装置110は、乱数値u2を暗号化して送信し、復号装置120は、暗号化された乱数値u2を復号するとしてもよい。

また、（c）及び（g）において、排他的論理和xorに代えて他の演算を用いるとしてもよい。例えば、（c）及び（g）において、それぞれ加算及び減算を用いてもよいし、また、乗算及び除算を用いてもよい。

（8）復号エラーの発生により暗号装置110と復号装置120との間で異なる共有鍵が導出されるのを防止するため、第1再暗号文c1'と第1暗号文c1とが同じである場合に、共有鍵K'を出力する代わりに、暗号装置110が乱数s、乱数値u、共有鍵Kのいずれか1つ以上について、ハッシュ関数値を生成し、生成したハッシュ関数値を復号装置120へ送信し、復号装置120がこのハッシュ関数値を検証することにより、共有鍵K'を出力するか否かを決定してもよい。例えば、このハッシュ関数値として、任意のハッシュ関数Hに対して、乱数sのハッシュ関数値H（s）を生成するようにしてもよいし、乱数s、乱数値u、共有鍵Kの組み合わせ、例えば、ハッシュ関数値H（s||u||k）やハッシュ関数値H（u||k）等を生成するようにしてもよい。

また、この場合、暗号装置110の第1関数部113は、関数値G（s）から乱数値uと共有鍵Kを導出する代わりに、G（s）から共有鍵Kのみを導出してもよい。

以下に、その具体例を述べる。

コンテンツ配信システム10は、暗号装置110及び復号装置120に代えて、暗号装置110b及び復号装置120bを含み、暗号装置110bは、図6に示すように、公開鍵入力部111、乱数生成部112、第1関数部113b、暗号化部114b、第1送信部117b、共通鍵暗号部118及び第2送信部119から構成されており、復号装置120は、図7に示すように、秘密鍵入力部121b、第1受信部122b、復号化部123b、第2関数部126b、比較部127b、共通鍵復号部128及び第2受信部129から構成される。比較部127bは、第3関数部127u及び比較演算部127vを含む。

暗号装置110bが乱数sのハッシュ関数値を生成し、復号装置120bがこのハッシュ関数値を検証する際に、暗号装置110bにおいて、図8の処理系統図に示すように、第1関数部113bは、G（s）を生成し（ステップS103）、G（s）からKを生成する（ステップS104）。

次に、暗号化部114bは、乱数値uを生成し、生成した乱数値uから乱数多項式rを生成し、乱数多項式r及び公開鍵多項式hを用いて乱数sの第1暗号文c1を生成し（ステップS105）、ハッシュ関数値H（s）を生成する（ステップS111）。

次に、第1送信部117bは、第1暗号文c1を送信し（ステップS106）、ハッシュ関数値H（s）を送信する（ステップS112）。

次に、復号装置１２０ｂにおいて、第１受信部１２２ｂは、第１暗号文ｃ１を受信し（ステップＳ１０６）、ハッシュ関数値Ｈ（ｓ）を受信する（ステップＳ１１２）。

次に、復号化部１２３ｂは、秘密鍵多項式ｆを用いて第１暗号文ｃ１を復号してｓ’を生成する（ステップＳ１５２）。

次に、第２関数部１２６は、Ｇ（ｓ’）を生成し（ステップＳ１５３）、Ｇ（ｓ’）からＫ’を生成する（ステップＳ１５４）。

次に、比較部１２７は、第３関数部１２７ｕにより、Ｈ（ｓ’）を生成し（ステップＳ１５４）、比較演算部１２７ｖにより、Ｈ（ｓ’）＝Ｈ（ｓ）が成立するかどうかチェックし（ステップＳ１６２）、成立すれば共有鍵Ｋ’を出力する（ステップＳ１５７）。

また、この場合、さらに安全性を高めるために、特許文献１に開示されている方法を用いて、乱数ｓに付加情報を附したものを暗号化して第１暗号文ｃ１を生成してもよい。すなわち、図６において、暗号化部１１４ｂは、付加情報Ｒａを生成し、ｓとＲａのビット結合ｓ｜｜Ｒａの値を暗号化して第１暗号文ｃ１を生成し、図７において、復号化部１２３ｂは、第１暗号文ｃ１を復号してｓ’｜｜Ｒａ’を生成し、Ｒａ’を除去して復号乱数ｓ’を生成してもよい。

また、特許文献１に開示されている通り、ｓ｜｜Ｒａの値の代わりに、ｓとＲａの可逆変換Ｆ（ｓ，Ｒａ）の値を用いてもよい。

２．実施の形態２

本発明に係る別の実施の形態としてのコンテンツ配信システム１０ｃ（図示していない）について説明する。

コンテンツ配信システム１０ｃは、コンテンツ配信システム１０を基本としてこれを変形したシステムであり、関数値Ｇ（ｓ）から乱数値ｕと共有鍵Ｋとの他にさらに検証値ａを生成する点と、暗号装置が、乱数ｓを暗号化した第１暗号文ｃ１を生成して送信する代わりに、検証値ａを暗号化した第１暗号文ｃ１と、乱数ｓを検証値ａに基づいて暗号化した第２暗号文ｃ２とを生成して送信する点において、コンテンツ配信システム１０と異なる。

以下、コンテンツ配信システム１０ｃについて、上記差異点を中心に詳しく説明する。

２．１　コンテンツ配信システム１０ｃの構成

コンテンツ配信システム１０ｃは、コンテンツ配信システム１０と同様の構成を有しており、暗号装置１１０及び復号装置１２０に代えて、暗号装置１１０ｃ及び復号装置１２０ｃを含んでいる。その他の構成については、コンテンツ配信システム１０におけるものと同様であるので説明を省略する。

２．２　暗号装置１１０ｃの構成

暗号装置１１０ｃは、図９に示すように、暗号装置１１０と同様の構成を有しており、乱数生成部１１２、第１関数部１１３、暗号化部１１４及び第１送信部１１７に代えて、乱数

生成部１１２ｃ、第１関数部１１３ｃ、暗号化部１１４ｃ、乱数マスク部１１６ｃ及び第１送信部１１７ｃを含む。

ここでは、乱数生成部１１２ｃ、第１関数部１１３ｃ、暗号化部１１４ｃ、乱数マスク部１１６ｃ及び第１送信部１１７ｃについて説明する。

（１）乱数生成部１１２ｃ

乱数生成部１１２ｃは、共有鍵Ｋを生成するための元となるシード値として、乱数ｓを生成し、生成した乱数ｓを第１関数部１１３ｂと乱数マスク部１１６ｃとへ出力する。

（２）第１関数部１１３ｃ

第１関数部１１３ｃは、乱数生成部１１２ｃから乱数ｓを受け取り、乱数ｓの関数値Ｇ（ｓ）を生成する。次に、生成した関数値Ｇ（ｓ）から検証値ａと共有鍵Ｋと乱数値ｕとを生成する。

ここで、関数Ｇは、出力長が３ｋビットのハッシュ関数であり、第１関数部１１３ｃは、関数値Ｇ（ｓ）の上位ｋビットを検証値ａとし、関数値Ｇ（ｓ）の中間のｋビットを共有鍵Ｋとし、関数値Ｇ（ｓ）の下位ｋビットを乱数値ｕとする。

次に、第１関数部１１３ｃは、生成した検証値ａと乱数値ｕとを暗号化部１１４ｃへ出力し、生成した共有鍵Ｋを共通鍵暗号部１１８へ出力し、生成した検証値ａを乱数マスク部１１６ｃへ出力する。

（３）暗号化部１１４ｃ

暗号化部１１４ｃは、公開鍵入力部１１１から公開鍵多項式ｈを受け取り、第１関数部１１３ｃから検証値ａと乱数値ｕとを受け取り、次に示すようにして、公開鍵多項式ｈと乱数値ｕとを用いて検証値ａの第１暗号文ｃ１を生成する。ここでは、第１暗号文ｃ１はＮＴＲＵ暗号による暗号文である。

暗号化部１１４ｃは、ＮＴＲＵ暗号のパラメータｄに対し、ｄ個の項の各係数が「１」であり、他のｄ個の項の各係数が「－１」であり、残りの項の各係数が「０」となる乱数多項式ｒを乱数値ｕから一意に求まるように生成する。具体的には、乱数値ｕを擬似乱数系列の初期値（乱数シード）として設定し、{０，１，．．．．，Ｎ－１}から重複しないように２ｄ個の擬似乱数を選択し、最初のｄ個の擬似乱数により示される次元の項の係数を「１」とし、他のｄ個の擬似乱数により示される次元の係数を「－１」とし、残りの項の係数を「０」とすることにより、乱数多項式ｒを生成する。

次に、受け取った検証値ａがＮＴＲＵ暗号の暗号アルゴリズムＥに適用できるように、暗号化部１１４ｃは、検証値ａを２進数表現した場合におけるＮ桁のビット列の各桁の値が、検証値多項式ａｐの各項の係数に対応するように、検証値多項式ａｐを構成することにより、検証値ａを検証値多項式ａｐに変換する。例えば、検証値ａの下位ｂビット目の値は、項Ｘ＾ｂの係数の値となる。具体的には、検証値ａ＝１００１０（ビット表現）の場合、検証値

多項式ａｐ＝Ｘ＾５＋Ｘ＾２を生成する。

次に、暗号化部１１４ｃは、公開鍵多項式ｈを鍵として使用して、乱数多項式ｒを用いて検証値多項式ａｐに前記暗号アルゴリズムＥを施して、暗号文多項式である第１暗号文ｃ１＝Ｅ（ａｐ，ｒ，ｈ）を生成する。

次に、暗号化部１１４ｃは、生成した第１暗号文ｃ１を第１送信部１１７ｃへ出力する。

（４）乱数マスク部１１６ｃ

乱数マスク部１１６ｃは、乱数生成部１１２ｃから乱数ｓを受け取り、第１関数部１１３ｃから検証値ａを受け取り、次に、第２暗号文ｃ２＝ｓ　ｘｏｒ　ａを生成し、生成した第２暗号文ｃ２を第１送信部１１７ｃへ出力する。

ここで、ｘｏｒは排他的論理和演算を表す演算子である。

なお、乱数マスク部１１６ｃは、排他的論理和に代えて、共有鍵暗号アルゴリズム、加算又は乗算を用いるとしてもよい。

（５）第１送信部１１７ｃ

第１送信部１１７ｃは、暗号化部１１４ｃから第１暗号文ｃ１を受け取り、乱数マスク部１１６ｃから第２暗号文ｃ２を受け取り、受け取った第１暗号文ｃ１と第２暗号文ｃ２とを、インターネット１３０を介して復号装置１２０ｃへ送信する。

２．２　復号装置１２０ｃの構成

復号装置１２０ｃは、図１０に示すように、復号装置１２０と同様の構成を有しており、第１受信部１２２、復号化部１２３、第２関数部１２６及び比較部１２７に代えて、第１受信部１２２ｃ、復号化部１２３ｃ、乱数マスク除去部１２５ｃ、第２関数部１２６ｃ及び比較部１２７ｃを含む。

ここでは、第１受信部１２２ｃ、復号化部１２３ｃ、乱数マスク除去部１２５ｃ、第２関数部１２６ｃ及び比較部１２７ｃについて説明する。

（１）第１受信部１２２ｃ

第１受信部１２２ｃは、インターネット１３０を介して、暗号装置１１０ｃから第１暗号文ｃ１と第２暗号文ｃ２とを受け取り、受け取った第１暗号文ｃ１を復号化部１２３ｃへ出力し、受け取った第２暗号文ｃ２を乱数マスク除去部１２５ｃへ出力する。

（２）復号化部１２３ｃ

復号化部１２３ｃは、秘密鍵入力部１２１から秘密鍵多項式ｆを受け取り、第１受信部１２２ｃから第１暗号文ｃ１を受け取り、次に示すようにして、秘密鍵多項式ｆを用いて、第１暗号文ｃ１を復号して復号検証値ａ’を生成する。ここでは、復号検証値ａ’はＮＴＲＵ暗号による復号文である。

復号化部１２３ｃは、秘密鍵多項式ｆを鍵として使用して、第１暗号文ｃ１に前記復号アルゴリズムＤを施して、復号検証値多項式ａｐ’＝Ｄ（ｃ１，ｆ）を生成する。ここで、復号

検証値多項式ａｐ’は、ＮＴＲＵ暗号の復号文であり多項式で表現されているので、復号化部１２３ｃは、復号検証値多項式ａｐ’の各項の係数が、２進数表現されたＮ桁のビット列である復号検証値ａ’の各桁の値に対応するように、復号検証値多項式ａｐ’を復号検証値ａ’に変換する。例えば、復号検証値多項式ａｐ’のｂ次元の項Ｘ＾ｂの係数を、復号検証値ａ’の下位ｂビット目の値とする。具体的には、復号検証値多項式ａｐ’＝Ｘ＾５＋Ｘ＾２の場合、復号検証値ａ’＝１００１０（ビット表現）に変換する。

次に、復号化部１２３ｃは、生成した復号検証値ａ’を乱数マスク除去部１２５ｃへ出力し、受け取った第１暗号文ｃ１を比較部１２７ｃへ出力する。

（３）乱数マスク除去部１２５ｃ

乱数マスク除去部１２５ｃは、第１受信部１２２ｃから第２暗号文ｃ２を受け取り、復号化部１２３ｃから復号検証値ａ’を受け取り、
復号乱数ｓ’＝ｃ２　ｘｏｒ　ａ’を生成し、生成した復号乱数ｓ’を第２関数部１２６ｃへ出力する。

なお、乱数マスク部１１６ｃが、排他的論理和に代えて、共有鍵暗号アルゴリズム、加算又は乗算を用いる場合において、乱数マスク除去部１２５ｃは、それぞれ、共有鍵暗号アルゴリズムに対応する共有鍵復号アルゴリズム、減算、又は除算を用いるとしてもよい。

（４）第２関数部１２６ｃ

第２関数部１２６ｃは、第１関数部１１３ｃが有する関数と同じ関数Ｇによるアルゴリズムを有している。

第２関数部１２６ｃは、乱数マスク除去部１２５ｃから復号乱数ｓ’を受け取り、受け取った復号乱数ｓ’の関数値Ｇ（ｓ’）を生成する。次に、第１関数部１１３ｃと同様にして、関数値Ｇ（ｓ’）から検証値ａ’’と共有鍵Ｋ’と乱数値ｕ’とを生成し、生成した検証値ａ’’と共有鍵Ｋ’と乱数値ｕ’とを比較部１２７ｃへ出力する。

（５）比較部１２７ｃ

比較部１２７ｃは、図１０に示すように、比較演算部１２７ｓ及び暗号化部１２７ｔから構成されている。

暗号化部１２７ｔは、秘密鍵入力部１２１から公開鍵多項式ｈを受け取り、第２関数部１２６ｃから検証値ａ’’と乱数値ｕ’とを受け取り、受け取った公開鍵多項式ｈと乱数値ｕ’を用いて、暗号化部１１４ｃと同様にして検証値ａ’’を暗号化して第１再暗号文ｃ１’を生成し、生成した第１再暗号文ｃ１’を比較演算部１２７ｓへ出力する。

また、比較演算部１２７ｓは、第２関数部１２６ｃから共有鍵Ｋ’を受け取り、復号化部１２３ｃから第１暗号文ｃ１を受け取り、暗号化部１２７ｔから第１再暗号文ｃ１’を受け取り、次に、受け取った第１暗号文ｃ１と、受け取った第１再暗号文ｃ１’とを比較し、第１暗号文ｃ１＝第１再暗号文ｃ１’であると判断する場合に、受け取った共有鍵Ｋ’を共通

鍵復号部１２８へ出力する。

２．３　コンテンツ配信システム１０ｃの動作

以下に、実施の形態２におけるコンテンツ配信システム１０ｃの全体の動作について、図１１に示す処理系統図を用いて、説明する。

暗号装置１１０ｃは、復号装置１２０ｃの公開鍵多項式ｈを受け取り（ステップＳ１０１）、乱数ｓを生成し（ステップＳ１０２）、関数値Ｇ（ｓ）を求め、関数値Ｇ（ｓ）から検証値ａ、共有鍵Ｋ及び乱数値ｕを導出する（ステップＳ１２１）。次に、暗号装置１１０ｃは、検証値ａを、公開鍵多項式ｈ及び乱数値ｕを用いてＮＴＲＵ暗号により暗号化して第１暗号文ｃ１を生成し（ステップＳ１０５）、検証値ａに基づき乱数ｓを暗号化して第２暗号文ｃ２＝ｓ　ｘｏｒ　ａを生成する（ステップＳ１２２）。次に、暗号装置１１０ｃは、第１暗号文ｃ１と第２暗号文ｃ２とをインターネット１３０を介して復号装置１２０ｃへ送信する（ステップＳ１０６）。

すなわち、この暗号装置１１０ｃは、以下の処理を行い、暗号文Ｃ＝（ｃ１，ｃ２）を復号装置１２０ｃへ送信する。

（ａ）乱数ｓを生成する。

（ｂ）Ｇ（ｓ）を生成し、Ｇ（ｓ）からａ、Ｋ、ｕを生成する。

（ｃ）公開鍵多項式ｈ、乱数値ｕを用いて検証値ａの第１暗号文ｃ１を生成する。

（ｄ）ｃ２＝ｓ　ｘｏｒ　ａを生成する。

次に、暗号装置１１０ｃは、導出した共有鍵Ｋを用いて、コンテンツサーバ装置１４０から受け取った平文ｍｉ（$1 \leqq i \leqq n$）を共通鍵暗号方式により暗号化して暗号文Ｃｉ（$1 \leqq i \leqq n$）を生成し（ステップＳ１０７）、インターネット１３０を介して復号装置１２０ｃへ送信する（ステップＳ１０８）。

一方、復号装置１２０ｃは、復号装置１２０ｃの秘密鍵多項式ｆ及び公開鍵多項式ｈを受け取り（ステップＳ１５１）、インターネット１３０を介して暗号装置１１０ｃから第１暗号文ｃ１と第２暗号文ｃ２を受信し（ステップＳ１０６）、第１暗号文ｃ１を秘密鍵多項式ｆを用いて復号して復号検証値ａ’を生成する（ステップＳ１５２）。次に、復号検証値ａ’に基づき第２暗号文ｃ２を復号して、復号乱数ｓ’＝ｃ２　ｘｏｒ　ａ’を生成する（ステップＳ１７１）。次に、復号装置１２０ｃは、復号乱数ｓ’の関数値Ｇ（ｓ’）から検証値ａ’’、共有鍵Ｋ’及び乱数値ｕ’を導出する（ステップＳ１７２）。さらに、検証値ａ’’を暗号化して第１再暗号文ｃ１’を生成し（ステップＳ１５５）、ｃ１’＝ｃ１であれば（ステップＳ１５６）、共有鍵Ｋ’を出力する（ステップＳ１５７）。

すなわち、この復号装置１２０ｃは、以下の処理を行い、共有鍵Ｋ’を導出する。

（ａ）秘密鍵多項式ｆを用いて第１暗号文ｃ１を復号してａ’を生成する。

（ｂ）ｓ’＝ｃ２　ｘｏｒ　ａ’を生成する。

（c）G（s'）を生成し、G（s'）からa''、K'、u'を生成する。

（d）公開鍵多項式h、乱数値u'を用いてa''の第1再暗号文c1'を生成する。

（e）c1'＝c1が成立するかどうかチェックする。成立すれば共有鍵K'を出力する。

ここで、暗号装置110cで用いられた公開鍵多項式hに対応する正しい秘密鍵多項式fが復号装置120cで用いられれば、第1暗号文c1は正しく復号されて、復号検証値a'＝aとなり、第2暗号文c2とa'から生成される復号乱数s'＝sとなる。従って、G（s'）から導出される検証値a''＝aとなり、共有鍵K'＝Kとなり、乱数値u'＝uとなる。こうして、a''＝a及びu'＝uが成り立つので、c1'＝c1が成り立ち、復号装置120cは暗号装置110cと同じ共有鍵Kを導出できることになる。

次に、復号装置120cは、インターネット130を介して暗号装置110cから共通鍵暗号文Ci（1≦i≦n）を受信し（ステップS108）、導出した共有鍵K'（＝K）を用いて、受信した共通鍵暗号文Ci（1≦i≦n）を共通鍵暗号方式により復号して復号文mi'（1≦i≦n）を生成し（ステップS158）、復号文mi'（1≦i≦n）を再生装置150へ出力する。

ここで、共通鍵暗号文生成時に用いた暗号鍵Kと復号文生成時に用いる暗号鍵K'とは同一であるので、復号装置120cは、正しい復号文mi'=mi（1≦i≦n）を得ることができる。

なお、復号エラーが発生した場合には、復号検証値a'と検証値aとは異なるので、第2暗号文c2から得られる復号乱数s'はsと異なる。従って、G（s'）から導出される乱数値u'及び共有鍵K'は、それぞれu、Kとは異なる。しかし、この場合、a'、u'がそれぞれa、uと異なるために第1再暗号文c1'は第1暗号文c1と異なるので、復号装置120cは、共有鍵K'を出力しない。

2．4　実施の形態2における効果

従来のRSA－KEMアルゴリズムでは、秘密鍵を知らなければ暗号文Cから導出できない要素sをハッシュ関数Gに入力して共有鍵Kを導出する。しかしながら、NTRU暗号を用いて、鍵カプセル化メカニズムであるRSA－KEMアルゴリズムを適用して共有鍵の配送を行おうとすると、復号エラーが発生する場合があるため、秘密鍵を用いても要素sが導出できず、従って正しくない共有鍵K'を導出する場合がある。

しかしながら、実施の形態2のコンテンツ配信システム、暗号装置及び復号装置は、乱数sのハッシュ関数値G（s）から共有鍵に加えて検証値aと乱数値uとを生成し、復号装置が乱数値uと公開鍵多項式hとを用いて復号検証値a'を再暗号化して第1再暗号文c1'を生成し、第1再暗号文c1'が第1暗号文c1と同じ値でない限り共有鍵Kを出力しないので、復号エラーが発生した場合、暗号装置と復号装置との間で異なる鍵が導出されるのを防止できる。

また、本発明による方式は、非特許文献３に記述されている証明方法と同様の方法により、理論的にその安全性が証明できる。

２．５　変形例

上記に説明した実施の形態２は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その主旨を逸脱しない範囲において種々なる態様で実施し得るものである。実施の形態１におけるのと同様の変形を施すことができるのはもちろんであるが、以下のような場合も本発明に含まれる。

（１）検証値ａから検証値多項式ａｐへの変換は、他の変換方法でもよい。例えば、ビット列の各ビットの値と多項式の各項の係数とを１対１に対応させる関数を用いて変換してもよいし、また、ビット列の各ビットの値と多項式の各項の係数とを１対１に対応させて記憶している関数値テーブルを用いて変換してもよい。

また、乱数値ｕから乱数多項式ｒへの変換は、他の変換方法でもよい。例えば、ｕからｒが一意に求まり、ｄ個の次元の項の係数を「１」とし、ｄ個の次元の項の係数を「－１」とし、他の次元の項の係数は「０」となるようにすれば、他の変換方法でもよい。例えば、乱数値ｕを多項式に対応させる関数、又は関数値テーブルを用いて変換してもよい。

（２）暗号化部１１４ｃ及び復号化部１２３ｃで用いる公開鍵暗号は、暗号化部１１４ｃにおいて、検証値ａを公開鍵と乱数値ｕを用いて暗号化して第１暗号文ｃ１を生成し、復号化部１２３ｃにおいて、第１暗号文ｃ１を秘密鍵で復号して、検証値ａと等しい復号検証値ａ’を生成できればよい。従って、暗号化部１１４ｃ及び復号化部１２３ｃで用いる公開鍵暗号は、ＮＴＲＵ暗号以外に、乱数を用いる公開鍵暗号ならばどんな暗号であってもよい。

例えば、ＥｌＧａｍａｌ暗号ならば、ｈ、ｆをそれぞれＥｌＧａｍａｌ暗号の公開鍵、秘密鍵とし、暗号化部１１４ｃにおいて、ａをｈと乱数値ｕを用いて暗号化してｃ１を生成し、復号化部１２３ｃにおいて、ｃ１をｆを用いて復号してａ’を生成すればよい。

（３）乱数値ｕは、第１関数部１１３ｃ及び第２関数部１２６ｃで生成される以外にも、暗号装置１１０ｃと復号装置１２０ｃとで同じ値を得られれば、他の生成方法でもよい。

例えば、任意の関数Ｆｕｎｃに対し、ｕ＝Ｆｕｎｃ（ｓ）として暗号装置１１０ｃと復号装置１２０ｃとで同じ値を得られるようにしてもよい。すなわち、

・Ｇ（ｓ）を生成し、Ｇ（ｓ）からａ、Ｋを生成する。

・Ｆｕｎｃ（ｓ）を生成し、ｕ＝Ｆｕｎｃ（ｓ）とする。

としてもよい。

（４）さらに、乱数値ｕについては、第１関数部１１３ｃ及び第２関数部１２６ｃで生成される以外にも、暗号装置１１０ｃと復号装置１２０ｃとで同じ値が得られればよいため、暗号装置１１０ｃが乱数値ｕを復号装置１２０ｃに直接送信してもよい。

すなわち、以下のように、暗号装置１１０ｃは、暗号文Ｃと乱数値ｕとを復号装置１２０

ｂに送信してもよい。また、乱数値ｕを暗号化して送信してもよい。

・Ｇ（ｓ）を生成し、Ｇ（ｓ）からａ、Ｋを生成する。

・暗号装置１１０ｃは、別途、乱数値ｕを、１２０ｂへ送信する。

（５）さらに、乱数値ｕについては、暗号装置１１０ｃと復号装置１２０ｃとで同じ値が得られればよいため、乱数値ｕの一部である部分情報を第１関数部１１３ｃ及び第２関数部１２６ｃで生成し、乱数値ｕの残りの部分情報を暗号装置１１０ｃから復号装置１２０ｃに直接送信してもよい。

例えば、以下のように、暗号装置１１０ｃは、暗号文Ｃと乱数値ｕ２を復号装置１２０ｃに送信してもよい。また、暗号装置１１０ｃは、乱数値ｕ２を暗号化して送信してもよい。

・Ｇ（ｓ）を生成し、Ｇ（ｓ）からａ、Ｋ、ｕ１を生成する。

・暗号装置１１０ｃは、別途、乱数値ｕ２を復号装置１２０ｃへ送信する。

・暗号装置１１０ｃは、乱数値ｕ＝ｕ１　ｘｏｒ　ｕ２を生成する。

（６）復号装置１２０ｃは、第１暗号文ｃ１が第２関数部１２６ｃで得られる検証値ａ''の暗号文かどうかチェックを行い、ｃ１がａ''の暗号文であるときに共有鍵Ｋ'を用いて共通鍵暗号文Ｃｉを復号しているが、第１暗号文ｃ１が復号検証値ａ'の暗号文かどうかをチェックしてもよい。

（７）復号装置１２０ｃは、第１暗号文ｃ１が第２関数部１２６ｃで得られる検証値ａ''の暗号文かどうかチェックを行い、ｃ１がａ''の暗号文であるときに共有鍵Ｋ'を用いて共通鍵暗号文Ｃｉを復号しているが、図１２の処理系統図のステップＳ１５６に示すように、比較部１２７ｃにおいて、復号化部１２３ｃが復号したａ'の値と第２関数部１２６ｃが生成したａ''の値が等しいかどうかをチェックしてもよい。

（８）復号エラー発生により暗号装置１１０ｃと復号装置１２０ｃとの間で異なる鍵が導出されるのを防止するため、第１再暗号文ｃ１'が第１暗号文ｃ１と同じ値かどうかを検証して共有鍵Ｋ'を出力する代わりに、暗号装置１１０ｃが乱数ｓ、検証値ａ、乱数値ｕ、共有鍵Ｋのいずれか１つ以上について、ハッシュ関数値を生成し、生成したハッシュ関数値を復号装置１２０ｃへ送信し、復号装置１２０ｃがこのハッシュ関数値を検証して共有鍵Ｋ'を出力するか否かを決定してもよいし、安全性を高めるために、特許文献１に開示されている方法を用いてもよい。すなわち、実施の形態１の変形例（８）を適用してもよい。

３．実施の形態１及び実施の形態２のまとめ

以上説明したように、本発明は、共有鍵データと、予め与えられた公開鍵データに基づいて前記共有鍵データを暗号化した暗号化共有鍵データを出力する共有鍵生成装置であって、秘密数データを生成する秘密数データ生成部と、前記秘密数データを所定の処理に基づいて乱数データと前記共有鍵データに変換する共有鍵導出部と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して暗号化共有鍵データを生成する第１の暗号化

部とを備える。

また、本発明は、共有鍵データと、予め与えられた公開鍵データに基づいて前記共有鍵データを暗号化した暗号化共有鍵データを出力する共有鍵生成装置であって、秘密数データを生成する秘密数データ生成部と、前記秘密数データを所定の処理に基づいて検証値データと乱数データと前記共有鍵データに変換する共有鍵導出部と、前記検証値データを前記公開鍵データと前記乱数データに基づいて暗号化して第１の暗号予備データを生成する第１の暗号化部と、前記秘密数データを前記検証値データに基づいて暗号化して第２の暗号予備データを生成する第２の暗号化部とを備え、前記暗号化共有鍵データは、前記第１の暗号予備データと前記第２の暗号予備データから構成される。

ここで、前記第２の暗号化部は、前記秘密数データと前記検証値データの排他的論理和演算を行って前記第２の暗号予備データを生成するとしてもよい。

ここで、前記第２の暗号化部は、前記秘密数データを、前記検証値データを暗号鍵として用いて共通鍵暗号方式により暗号化して前記第２の暗号予備データを生成するとしてもよい。

ここで、前記第２の暗号化部は、前記秘密数データに前記検証値データを加算して前記第２の暗号予備データを生成するとしてもよい。

ここで、前記第２の暗号化部は、前記秘密数データに前記検証値データを乗算して前記第２の暗号予備データを生成するとしてもよい。

ここで、前記暗号化共有鍵データは、前記第１の暗号予備データと前記第２暗号予備データのビット連結データであるとしてもよい。

ここで、前記第１の暗号化部は、ＮＴＲＵ暗号方式により暗号化して前記暗号化共有鍵データを生成するとしてもよい。

ここで、前記第１の暗号化部は、ＮＴＲＵ暗号方式により暗号化して前記第１の暗号予備データを生成するとしてもよい。

ここで、前記秘密数データは、ランダムに生成される乱数であるとしてもよい。

ここで、前記共有鍵導出部は、所定の処理として、一方向性ハッシュ関数を用いるとしてもよい。

また、本発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記暗号化共有鍵データを前記秘密鍵データに基づいて復号化して秘密数データを生成する第１の復号化部と、前記秘密数データを所定の処理に基づいて乱数データと前記共有鍵データに変換する共有鍵導出部と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して再暗号化共有鍵データを生成する第３の暗号化部とを備え、前記暗号化共有鍵データと前記再暗号化共有鍵データが一致する場合に、前記共有鍵データを出力する。

また、本発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、第１の暗号

予備データと第２の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第１の復号化部と、前記第２の暗号予備データを前記検証値データに基づいて復号化して秘密数データを生成する第２の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出部と、前記検証値検証データを前記公開鍵データと前記乱数データに基づいて暗号化して第３の暗号予備データを生成する第３の暗号化部とを備え、前記第１の暗号予備データと前記第３の暗号予備データが一致する場合に、前記共有鍵データを出力する。

また、本発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、第１の暗号予備データと第２の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第１の復号化部と、前記第２の暗号予備データを前記検証値データに基づいて復号化して秘密数データを生成する第２の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出部と、前記検証値データを前記公開鍵データと前記乱数データに基づいて暗号化して第３の暗号予備データを生成する第３の暗号化部とを備え、前記第１の暗号予備データと前記第３の暗号予備データが一致する場合に、前記共有鍵データを出力する。

ここで、前記第２の復号化部は、前記第２の暗号予備データと前記検証値データの排他的論理和演算を行って前記秘密数データを生成するとしてもよい。

ここで、前記第２の復号化部は、前記第２の暗号予備データを、前記検証値データを暗号鍵として用いて共通鍵暗号方式により復号化して前記秘密数データを生成するとしてもよい。

ここで、前記第２の復号化部は、前記第２の暗号予備データに前記検証値データを減算して前記秘密数データを生成するとしてもよい。

ここで、前記第２の暗号化部は、前記第２の暗号予備データを前記検証値データで除算して前記秘密数データ第２の秘密数データを生成するとしてもよい。

ここで、前記第１の復号化部は、ＮＴＲＵ暗号方式により復号化して前記共有鍵データを生成するとしてもよい。

ここで、前記第１の復号化部は、ＮＴＲＵ暗号方式により復号化して前記検証値データを生成するとしてもよい。

ここで、前記共有鍵導出部は、所定の処理として、一方向性ハッシュ関数を用いるとしてもよい。

また、本発明は、予め与えられた公開鍵データに基づいて平文データを暗号化した暗号文データを生成する暗号装置であって、秘密数データを生成する秘密数データ生成部と、前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出部と、

前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第１の暗号予備データを生成する第１の暗号化部と、前記平文データを前記共有鍵データに基づいて暗号化して第２の暗号予備データを生成する第２の暗号化部とを備え、前記暗号文データは、前記第１の暗号予備データと前記第２の暗号予備データから構成される。

また、本発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、第１の暗号予備データと第２の暗号予備データから構成される暗号文データを復号して復号文データを出力する復号装置であって、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して秘密数データを生成する第１の復号化部と、前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出部と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第３の暗号予備データを生成する第３の暗号化部とを備え、前記第１の暗号予備データと前記第３の暗号予備データが一致する場合に、前記第２の暗号予備データを前記共有鍵に基づいて復号化して前記復号文データを生成する復号部とを備える。

また、本発明は、予め与えられた公開鍵データに基づいて平文データを暗号化した暗号文データを生成する暗号装置、及び予め与えられた秘密鍵データ及び公開鍵データに基づいて暗号文データを復号して復号文データを出力する復号装置からなる暗号システムである。前記暗号装置は、秘密数データを生成する秘密数データ生成部と、前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出部と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第１の暗号予備データを生成する第１の暗号化部と、前記平文データを前記共有鍵データに基づいて暗号化して第２の暗号予備データを生成する第２の暗号化部とを備え、前記暗号文データは、前記第１の暗号予備データと前記第２の暗号予備データと前記第３の暗号予備データから構成される。前記復号装置は、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して秘密数データを生成する第１の復号化部と、前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出部と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第３の暗号予備データを生成する第３の暗号化部とを備え、前記第１の暗号予備データと前記第３の暗号予備データが一致する場合に、前記第２の暗号予備データを前記共有鍵に基づいて復号化して前記復号文データを生成する復号部とを備える。

以上に説明したように、本発明は、従来システムにおける問題点を鑑みて行われたもので、暗号システムにおいて、ＮＴＲＵ暗号を適用できる新しい鍵カプセル化メカニズムを構成することで、暗号装置と復号装置との間で異なる鍵が導出されるのを防止でき、鍵カプセル化メカニズムにより導出される鍵を用いた送信装置から受信装置への確実な暗号化通信ができる。

以上により、従来技術では達成できなかった暗号システムを提供することができ、その価

値は大きい。

４．実施の形態３

本発明に係るさらに別の実施の形態としてのコンテンツ配信システム１０ｄ（図示していない）について説明する。

なお、コンテンツ配信システム１０ｄは、コンテンツ配信システム１０を変形したシステムである。ここでは、コンテンツ配信システム１０ｄについて、コンテンツ配信システム１０との差異点を中心に詳しく説明する。

４．１　コンテンツ配信システム１０ｄの構成

コンテンツ配信システム１０ｄは、コンテンツ配信システム１０と同様の構成を有しており、暗号装置１１０及び復号装置１２０に代えて、暗号装置１１０ｄ及び復号装置１２０ｄを含んでいる。その他の構成については、コンテンツ配信システム１０におけるものと同様であるので説明を省略する。

コンテンツ配信システム１０ｄは、ＮＴＲＵ暗号を用いて鍵カプセル化メカニズムによる鍵配送を行って暗号化通信を行う暗号通信システムであり、暗号装置１１０ｄと復号装置１２０ｄとは、インターネット１３０を介して接続されている。

４．２　暗号装置１１０ｄの構成

暗号装置１１０ｄは、図１３に示すように、公開鍵入力部１１１ｄ、乱数生成部１１２ｄ、第１関数部１１３ｄ、暗号化部１１４ｄ、第２関数部１１５ｄ、乱数マスク部１１６ｄ、第１送信部１１７ｄ、共通鍵暗号部１１８及び第２送信部１１９から構成されている。

暗号装置１１０ｄは、暗号装置１１０と同様のコンピュータシステムであり、マイクロプロセッサが、コンピュータプログラムに従って動作することにより、暗号装置１１０ｄは、その機能を達成する。

（１）公開鍵入力部１１１ｄ

公開鍵入力部１１１ｄは、メモリカード１６０から復号装置１２０の公開鍵多項式ｈを読み出し、読み出した公開鍵多項式ｈを暗号化部１１４ｄへ出力する。

（２）乱数生成部１１２ｄ

乱数生成部１１２ｄは、共有鍵Ｋを生成するための元となるシード値として、乱数ｓを生成し、生成した乱数ｓを第１関数部１１３と乱数マスク部１１６とへ出力する。

（３）第１関数部１１３ｄ

第１関数部１１３ｄは、乱数生成部１１２ｄから乱数ｓを受け取り、受け取った乱数ｓの関数値Ｇ（ｓ）を生成し、関数値Ｇ（ｓ）から検証値ａと共有鍵Ｋを生成する。ここでは、関数Ｇは、一方向性関数である出力長が２ｋビットのハッシュ関数であり、第１関数部１１３ｄは、Ｇ（ｓ）の上位ｋビットを検証値ａとし、Ｇ（ｓ）の下位ｋビットを共有鍵Ｋとする。

次に、第１関数部１１３ｄは、生成した検証値ａを暗号化部１１４ｄと第２関数部１１５ｄとへ出力し、生成した共有鍵Ｋを共通鍵暗号部１１８へ出力する。

（４）暗号化部１１４ｄ

暗号化部１１４ｄは、公開鍵入力部１１１ｄから公開鍵多項式ｈを受け取り、第１関数部１１３ｄから検証値ａを受け取り、次に示すようにして、受け取った公開鍵多項式ｈを用いて検証値ａの第１暗号文ｃ１を生成する。ここで、生成される第１暗号文ｃ１は、ＮＴＲＵ暗号による暗号文である。

暗号化部１１４ｄは、ＮＴＲＵ暗号のパラメータｄに対し、ｄ個の項の各係数が「１」であり、別のｄ個の項の各係数が「－１」であり、その他の項の各係数が「０」となる乱数多項式ｒをランダムに生成する。次に、検証値ａがＮＴＲＵ暗号の暗号アルゴリズムＥに適用できるように、検証値ａを２進数表現した場合のＮ桁のビット列の各桁の値が、検証値多項式ａｐの各項の係数に対応するように、検証値多項式ａｐを生成する。例えば、検証値ａの下位ｂビット目の値を、検証値多項式ａｐの項Ｘ＾ｂの係数とする。こうして、検証値ａを検証値多項式ａｐに変換する。具体的には、検証値ａ＝１００１０（ビット表現）の場合、検証値多項式ａｐ＝Ｘ＾５＋Ｘ＾２と変換する。次に、公開鍵多項式ｈを使用して、乱数多項式ｒを用いて検証値多項式ａｐに前記暗号アルゴリズムＥを施して、暗号文多項式である第１暗号文ｃ１＝Ｅ（ａｐ，ｒ，ｈ）を生成する。

次に、暗号化部１１４ｄは、生成した第１暗号文ｃ１を第２関数部１１５ｄと第１送信部１１７ｄとへ出力する。

（５）第２関数部１１５ｄ

第２関数部１１５ｄは、第１関数部１１３ｄから検証値ａを受け取り、暗号化部１１４ｄから第１暗号文ｃ１を受け取り、次に示すようにして、検証値ａと第１暗号文ｃ１の関数値Ｈ（ａ，ｃ１）を生成する。

ここでは、関数Ｈはハッシュ関数であり、一方向性関数の一種である。

第１暗号文ｃ１は、ＮＴＲＵ暗号の暗号文であり多項式で表現されているので、第２関数部１１５ｄは、第１暗号文ｃ１の各項の係数が、２進数表現した場合のＮ桁の第１暗号文ビット列ｃ１’の各桁の値に対応するように、第１暗号文ビット列ｃ１’を生成する。例えば、第１暗号文ｃ１のｂ次元の項Ｘ＾ｂの係数を、第１暗号文ビット列ｃ１’の下位ｂビット目の値とする。こうして、第１暗号文ｃ１を第１暗号文ビット列ｃ１’に変換する。具体的には、第１暗号文ｃ１＝Ｘ＾５＋Ｘ＾２の場合、第１暗号文ビット列ｃ１’＝１００１０（ビット表現）と変換する。

次に、第２関数部１１５ｄは、ハッシュ関数Ｈに検証値ａと第１暗号文ビット列ｃ１’とのビット結合ａ｜｜ｃ１’を入力して、関数値Ｈ（ａ，ｃ１）＝Ｈ（ａ｜｜ｃ１’）を生成する。ここで、「｜｜」は、ビット結合を示す演算子である。

次に、第２関数部１１５ｄは、生成した関数値Ｈ（ａ，ｃ１）を乱数マスク部１１６ｄへ出力する。

（６）乱数マスク部１１６ｄ

乱数マスク部１１６ｄは、乱数生成部１１２ｄから乱数ｓを受け取り、第２関数部１１５ｄから関数値Ｈ（ａ，ｃ１）を受け取る。次に、第２暗号文ｃ２＝ｓ　ｘｏｒ　Ｈ（ａ，ｃ１）を生成し、生成した第２暗号文ｃ２を第１送信部１１７ｄへ出力する。

なお、乱数マスク部１１６ｄは、排他的論理和ｘｏｒに代えて、共有鍵暗号アルゴリズム、加算又は乗算を用いるとしてもよい。

（７）第１送信部１１７ｄ

第１送信部１１７ｄは、暗号化部１１４ｄから第１暗号文ｃ１を受け取り、乱数マスク部１１６ｄから第２暗号文ｃ２を受け取り、受け取った第１暗号文ｃ１と第２暗号文ｃ２とを、インターネット１３０を介して、復号装置１２０ｄへ送信する。

（８）共通鍵暗号部１１８及び第２送信部１１９

共通鍵暗号部１１８及び第２送信部１１９は、以下に示す点を除いて、それぞれ、暗号装置１１０に含まれている共通鍵暗号部１１８及び第２送信部１１９と同じである。

共通鍵暗号部１１８は、第１関数部１１３ｄから共有鍵Ｋを受け取る。

４．３　復号装置１２０ｄの構成

復号装置１２０ｄは、図１４に示すように、秘密鍵入力部１２１ｄ、第１受信部１２２ｄ、復号化部１２３ｄ、第３関数部１２４ｄ、乱数マスク除去部１２５ｄ、第４関数部１２６ｄ、比較部１２７ｄ、共通鍵復号部１２８及び第２受信部１２９から構成されている。

復号装置１２０ｄは、復号装置１２０と同様のコンピュータシステムであり、マイクロプロセッサが、コンピュータプログラムに従って動作することにより、復号装置１２０ｄは、その機能を達成する。

なお、共通鍵復号部１２８及び第２受信部１２９は、それぞれ、復号装置１２０に含まれている共通鍵復号部１２８及び第２受信部１２９と同じであるので、ここでは、説明を省略する。

（１）秘密鍵入力部１２１ｄ

秘密鍵入力部１２１ｄは、メモリカード１７０から復号装置１２０ｄの秘密鍵多項式ｆを読み出し、読み出した秘密鍵多項式ｆを復号化部１２３ｄへ出力する。

（２）第１受信部１２２ｄ

第１受信部１２２ｄは、インターネット１３０を介して暗号装置１１０ｄから第１暗号文ｃ１と第２暗号文ｃ２とを受け取り、受け取った第１暗号文ｃ１を復号化部１２３ｄと第３関数部１２４ｄとへ出力し、受け取った第２暗号文ｃ２を乱数マスク除去部１２５ｄへ出力する。

なお、乱数マスク部１１６ｄが、排他的論理和に代えて、共有鍵暗号アルゴリズム、加算又は乗算を用いる場合において、乱数マスク除去部１２５ｄは、それぞれ、共有鍵暗号アルゴリズムに対応する共有鍵復号アルゴリズム、減算、又は除算を用いるとしてもよい。

（3）復号化部１２３ｄ

復号化部１２３ｄは、秘密鍵入力部１２１ｄから秘密鍵多項式ｆを受け取り、第１受信部１２２ｄから第１暗号文ｃ１を受け取り、次に示すようにして、秘密鍵多項式ｆを用いて、第１暗号文ｃ１を復号して復号検証値ａ’を生成する。ここでは、復号検証値ａ’はＮＴＲＵ暗号による復号文である。

復号化部１２３ｄは、秘密鍵多項式ｆを使用して、第１暗号文ｃ１に前記復号アルゴリズムＤを施して、復号検証値多項式ａｐ’＝Ｄ（ｃ１,ｆ）を生成する。次に、復号検証値多項式ａｐ’は、ＮＴＲＵ暗号の復号文であり多項式で表現されているので、復号化部１２３ｄは、復号検証値多項式ａｐ’の各係数が、復号検証値ａ’を２進数表現した場合のＮ桁のビット列の各桁の数に対応するように、復号検証値ａ’を生成する。例えば、復号検証値多項式ａｐ’のｂ次元の項Ｘ＾ｂの係数を、復号検証値ａ’の下位ｂビット目の値とする。こうして、復号検証値多項式ａｐ’を復号検証値ａ’に変換する。具体的には、復号検証値多項式ａｐ’＝Ｘ＾５＋Ｘ＾２の場合、復号検証値ａ’＝１００１０（ビット表現）に変換する。

次に、復号化部１２３ｄは、生成した復号検証値ａ’を第３関数部１２４ｄと比較部１２７ｄとへ出力する。

（4）第３関数部１２４ｄ

第３関数部１２４ｄは、第２関数部１１５ｄが有する関数と同じ関数Ｈのアルゴリズムを有している。

第３関数部１２４ｄは、第１受信部１２２ｄから第１暗号文ｃ１を受け取り、復号化部１２３ｄから復号検証値ａ’を受け取る。次に、第２関数部１１５ｄと同様にして、検証値ａ’と第１暗号文ｃ１との関数値Ｈ（ａ’，ｃ１）を生成し、生成した関数値Ｈ（ａ’，ｃ１）を乱数マスク除去部１２５ｄへ出力する。

（5）乱数マスク除去部１２５ｄ

乱数マスク除去部１２５ｄは、第１受信部１２２ｄから第２暗号文ｃ２を受け取り、第３関数部１２４ｄからハッシュ関数値Ｈ（ａ’，ｃ１）を受け取り、次に、復号乱数ｓ’＝ｃ２ｘｏｒ　Ｈ（ａ’，ｃ１）を生成し、生成した復号乱数ｓを第４関数部１２６ｄへ出力する。

（6）第４関数部１２６ｄ

第４関数部１２６ｄは、第１関数部１１３ｄが有する関数と同じ関数Ｇのアルゴリズムを有している。

第４関数部１２６ｄは、乱数マスク除去部１２５ｄから復号乱数ｓ’を受け取り、復号乱数ｓ’のハッシュ関数値Ｇ（ｓ’）を生成する。次に、第１関数部１１３ｄと同様にして、関

数値G（s'）から検証値a''と共有鍵K'とを生成し、生成した検証値a''と共有鍵K'とを比較部１２７ｄへ出力する。

（7）比較部１２７ｄ

比較部１２７ｄは、復号化部１２３ｄから復号検証値a'を受け取り、第４関数部１２６ｄから検証値a''と共有鍵K'とを受け取り、次に、復号検証値a'と検証値a''が等しいかどうかチェックを行い、復号検証値a'と検証値a''とが等しければ、共有鍵K'を共通鍵復号部１２８へ出力する。

（8）共通鍵復号部１２８及び第２受信部１２９

共通鍵復号部１２８は、比較部１２７ｄから共有鍵K'を受け取る。

その他の点については、共通鍵復号部１２８は、復号装置１２０に含まれている共通鍵復号部１２８と同じであるので、ここでは、説明を省略する。

また、第２受信部１２９は、復号装置１２０に含まれている第２受信部１２９と同じであるので、ここでは、説明を省略する。

４．４　コンテンツ配信システム１０ｄの動作

コンテンツ配信システム１０ｄの動作について、図１５に示すフローチャート及び図１６に示す処理系統図を用いて説明する。

公開鍵入力部１１１ｄは、メモリカード１６０から復号装置１２０ｄの公開鍵多項式ｈを受け取り、公開鍵多項式ｈを暗号化部１１４ｄへ出力する（ステップＳ２０１）。

次に、乱数生成部１１２ｄは、乱数ｓを生成して、乱数ｓを第１関数部１１３ｄと乱数マスク部１１６ｄとへ出力する（ステップＳ２０２）。

次に、第１関数部１１３ｄは、乱数生成部１１２ｄから乱数ｓを受け取り、乱数ｓの関数値G（ｓ）を生成する（ステップＳ２０３）。そして、第１関数部１１３ｄは、関数値G（ｓ）から検証値ａと共有鍵Ｋを生成して、検証値ａを暗号化部１１４ｄと第２関数部１１５ｄとへ出力し、共有鍵Ｋを共通鍵暗号部１１８へ出力する（ステップＳ２０４）。

次に、暗号化部１１４ｄは、公開鍵入力部１１１ｄから公開鍵多項式ｈを受け取り、第１関数部１１３ｄから検証値ａを受け取る。そして、暗号化部１１４ｄは、公開鍵多項式ｈを用いて検証値ａの第１暗号文ｃ１を生成し、第１暗号文ｃ１を第２関数部１１５ｄと第１送信部１１７ｄとへ出力する（ステップＳ２０５）。

次に、第２関数部１１５ｄは、第１関数部１１３ｄから検証値ａを受け取り、暗号化部１１４ｄから第１暗号文ｃ１を受け取り、検証値ａと第１暗号文ｃ１との関数値Ｈ（ａ，ｃ１）を生成し、関数値Ｈ（ａ，ｃ１）を乱数マスク部１１６へ出力する（ステップＳ２０６）。

次に、乱数マスク部１１６ｄは、乱数生成部１１２ｄから乱数ｓを受け取り、第２関数部１１５ｄから関数値Ｈ（ａ，ｃ１）を受け取り、乱数マスク部１１６ｄは、第２暗号文ｃ２＝ｓ　ｘｏｒ　Ｈ（ａ，ｃ１）を生成し、第２暗号文ｃ２を第１送信部１１７ｄへ出力する

（ステップＳ２０７）。

次に、第１送信部１１７ｄは、暗号化部１１４ｄから第１暗号文ｃ１を受け取り、乱数マスク部１１６ｄから第２暗号文ｃ２を受け取り、第１暗号文ｃ１と第２暗号文ｃ２とをインターネット１３０を介して復号装置１２０ｄへ送信する（ステップＳ２０８）。

次に、共通鍵暗号部１１８は、コンテンツサーバ装置１４０から複数の平文ｍｉ（１≦ｉ≦ｎ）を受け取り、第１関数部１１３ｄから共有鍵Ｋを受け取り、共有鍵Ｋを使用して平文ｍｉ（１≦ｉ≦ｎ）に共通鍵暗号アルゴリズムＳｙｍを施して、共通鍵暗号文Ｃｉ＝Ｓｙｍ（ｍｉ，Ｋ）（１≦ｉ≦ｎ）を生成し、共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を第２送信部１１９へ出力する（ステップＳ２０９）。

次に、第２送信部１１９は、共通鍵暗号部１１８から共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を受け取り、インターネット１３０を介して復号装置１２０ｄへ送信し（ステップＳ２１０）、処理を終了する。

一方、秘密鍵入力部１２１ｄは、メモリカード１７０から復号装置１２０ｄの秘密鍵多項式ｆを受け取り、秘密鍵多項式ｆを復号化部１２３へ出力する（ステップＳ２５１）。

次に、第１受信部１２２ｄは、インターネット１３０を介して暗号装置１１０ｄから第１暗号文ｃ１と第２暗号文ｃ２とを受け取り、第１暗号文ｃ１を復号化部１２３ｄと第３関数部１２４ｄとへ出力し、第２暗号文ｃ２を乱数マスク除去部１２５ｄへ出力する（ステップＳ２０８）。

次に、復号化部１２３ｄは、秘密鍵入力部１２１から秘密鍵多項式ｆを受け取り、第１受信部１２２ｄから第１暗号文ｃ１を受け取り、次に、秘密鍵多項式ｆを用いて、第１暗号文ｃ１を復号して復号検証値ａ’を生成し、復号検証値ａ’を第３関数部１２４ｄと比較部１２７ｄへ出力する（ステップＳ２５２）。

次に、第３関数部１２４ｄは、第１受信部１２２ｄから第１暗号文ｃ１を受け取り、復号化部１２３ｄから復号検証値ａ’を受け取り、次に、第２関数部１１５ｄと同様にして、検証値ａ’と第１暗号文ｃ１の関数値Ｈ（ａ’，ｃ１）を生成し、関数値Ｈ（ａ’，ｃ１）を乱数マスク除去部１２５ｄへ出力する（ステップＳ２５３）。

次に、乱数マスク除去部１２５ｄは、第１受信部１２２ｄから第２暗号文ｃ２を受け取り、第３関数部１２４ｄからハッシュ関数値Ｈ（ａ’，ｃ１）を受け取り、次に、復号乱数ｓ’＝ｃ２　ｘｏｒ　Ｈ（ａ’，ｃ１）を生成し、復号乱数ｓを第４関数部１２６ｄへ出力する（ステップＳ２５４）。

次に、第４関数部１２６ｄは、乱数マスク除去部１２５から復号乱数ｓ’を受け取り、復号乱数ｓ’のハッシュ関数値Ｇ（ｓ’）を生成し（ステップＳ２５５）、第１関数部１１３ｄと同様にして、関数値Ｇ（ｓ’）から検証値ａ’’と共有鍵Ｋ’とを生成して、検証値ａ’’と共有鍵Ｋ’とを比較部１２７ｄへ出力する（ステップＳ２５６）。

次に、比較部１２７ｄは、復号化部１２３から復号検証値ａ’を受け取り、第４関数部１２６ｄから検証値ａ’’と共有鍵Ｋ’とを受け取り、復号検証値ａ’と検証値ａ’’とが等しいかどうかチェックを行い、等しくなければ（ステップＳ２５７）、処理を終了する。

復号検証値ａ’と検証値ａ’’とが等しければ（ステップＳ２５７）、比較部１２７ｄは、共有鍵Ｋ’を共通鍵復号部１２８へ出力する（ステップＳ２５８）。

次に、第２受信部１２９は、インターネット１３０を介して暗号装置１１０ｄから暗号文Ｃｉ（１≦ｉ≦ｎ）を受信し、共通鍵復号部１２８へ出力する（ステップＳ２１０）。

次に、共通鍵復号部１２８は、比較部１２７ｄから共有鍵Ｋ’を受け取り、第２受信部１２９から共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を受け取り、共有鍵Ｋ’を使用して共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）に共通鍵暗号アルゴリズムＳｙｍを施して、復号文ｍｉ’＝Ｓｙｍ（Ｃｉ，Ｋ）（１≦ｉ≦ｎ）を生成し、復号文ｍｉ’（１≦ｉ≦ｎ）を外部へ出力し（ステップＳ２５９）、処理を終了する。

４．５　コンテンツ配信システム１０ｄの動作検証

以下に、コンテンツ配信システム１０ｄの全体の動作について説明する。

暗号装置１１０ｄは、復号装置１２０ｄの公開鍵多項式ｈを入力とし、乱数ｓを生成して、関数値Ｇ（ｓ）から検証値ａと共有鍵Ｋを導出する。次に、暗号装置１１０ｄは、検証値ａを公開鍵多項式ｈを用いてＮＴＲＵ暗号で暗号化して第１暗号文ｃ１を生成し、検証値ａと第１暗号文ｃ１から関数値Ｈ（ａ，ｃ１）を生成し、乱数ｓと関数値Ｈ（ａ，ｃ１）から第２暗号文ｃ２＝ｓ　ｘｏｒ　Ｈ（ａ，ｃ１）を生成する。次に、暗号装置１１０ｄは、第１暗号文ｃ１と第２暗号文ｃ２をインターネット１３０を介して復号装置１２０ｄへ送信する。

すなわち、この暗号装置１１０ｄは、以下の処理を行い、暗号文Ｃ＝（ｃ１，ｃ２）を復号装置１２０ｄへ送信する。

・乱数ｓを生成する。

・Ｇ（ｓ）を生成し、Ｇ（ｓ）からａ，Ｋを生成する。

・公開鍵多項式ｈを用いて検証値ａの第１暗号文ｃ１を生成する。

・ｃ２＝ｓ　ｘｏｒ　Ｈ（ａ，ｃ１）を生成する。

・共有鍵Ｋと暗号文Ｃ＝（ｃ１，ｃ２）を出力する。

次に、暗号装置１１０ｄは、導出した共有鍵Ｋを用いて、コンテンツサーバ装置１４０から入力された平文ｍｉ（１≦ｉ≦ｎ）を共通鍵暗号で暗号化して暗号文Ｃｉ（１≦ｉ≦ｎ）を生成し、インターネット１３０を介して復号装置１２０ｄへ送信する。

一方、復号装置１２０ｄは、復号装置１２０ｄの秘密鍵多項式ｆを入力とし、インターネット１３０を介して暗号装置１１０ｄから第１暗号文ｃ１と第２暗号文ｃ２とを受信し、第１暗号文ｃ１を秘密鍵多項式ｆを用いて復号して復号検証値ａ’を生成する。復号検証値ａ’と第１暗号文ｃ１から関数値Ｈ（ａ’，ｃ１）を生成し、第２暗号文ｃ２と関数値Ｈ（ａ’，

ｃ１）から復号乱数ｓ’＝ｃ２　ｘｏｒ　Ｈ（ａ’，ｃ１）を生成する。次に、復号装置１２０ｄは、復号乱数ｓ’の関数値Ｇ（ｓ’）から検証値ａ’’と共有鍵Ｋ’を導出し、検証値ａ’’＝ａ’であれば共有鍵Ｋ’を出力する。

すなわち、この復号装置１２０ｄは、以下の処理を行い、共有鍵Ｋ’を導出する。

・秘密鍵多項式ｆを用いて第１暗号文ｃ１を復号してａ’を生成する。

・ｓ’＝ｃ２　ｘｏｒ　Ｈ（ａ’，ｃ１）を生成する。

・Ｇ（ｓ’）を生成し、Ｇ（ｓ’）からａ’’，Ｋ’を生成する。

・ａ’’＝ａ’が成立するかどうかチェックする。成立すれば共有鍵Ｋ’を出力する。

ここで、暗号装置１１０ｄで用いられた公開鍵多項式ｈに対応する正しい秘密鍵多項式ｆが復号装置１２０ｄで用いられれば、第１暗号文ｃ１は正しく復号されて、復号検証値ａ’＝ａとなり、第２暗号文ｃ２とＨ（ａ’，ｃ１）から生成される復号乱数ｓ’＝ｓとなる。従って、Ｇ（ｓ’）から導出される検証値ａ’’＝ａとなり、共有鍵Ｋ’＝Ｋとなる。そして、ａ’’＝ａ’が成り立つので、復号装置１２０ｄは暗号装置１１０ｄと同じ共有鍵Ｋを導出できることになる。

次に、復号装置１２０ｄは、導出した共有鍵Ｋ’（＝Ｋ）を用いて、インターネット１３０を介して暗号装置１１０ｄから共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を受け取り、受け取った共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を共通鍵暗号で復号して復号文ｍｉ’（１≦ｉ≦ｎ）を生成して再生装置１５０へ出力する。

ここで、共通鍵暗号文生成時に用いた暗号鍵Ｋと復号文生成時に用いる暗号鍵Ｋ’は同一であるので、復号装置１２０ｄは、正しくｍｉ’＝ｍｉ（１≦ｉ≦ｎ）を得ることができる。

４．６　実施の形態３における効果

従来のＰＳＥＣ－ＫＥＭアルゴリズムでは、ハッシュ関数Ｈの入力にａ＊Ｐ，ａ＊Ｗを用い、秘密鍵を用いずにａ＊Ｐからａ＊Ｗを計算することが困難なＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題を用いて、最終的に共有鍵Ｋを導出することにより、秘密鍵を知らなければその共有鍵Ｋを導出できないようにしている。従って、ＮＴＲＵ暗号をはじめ、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題を利用しない他の公開鍵暗号は、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題のａ＊Ｐ、ａ＊Ｗに相当するものがないため、ＰＳＥＣ－ＫＥＭアルゴリズムを適用できないという問題点がある。

しかしながら、本発明のコンテンツ配信システム、暗号装置及び復号装置は、ハッシュ関数Ｈの入力を検証値ａとその暗号文ｃ１としているので、ＰＳＥＣ－ＫＥＭアルゴリズムを適用して、ＮＴＲＵ暗号や他の公開鍵暗号を利用できる。

なお、ＮＴＲＵ暗号では、公開鍵を用いて平文を暗号化して暗号文を生成し、正規の秘密鍵を用いて暗号文を復号して復号文を生成しても、復号文が元の平文と異なる場合が発生す

る（例えば、非特許文献２参照。）。このような復号エラーが発生すると、復号装置は誤った復号検証値ａ’を得ることになるが、Ｇ（ｓ’）から得られる検証値ａ’’はａ’と等しくならないために、共有鍵Ｋ’を出力しない。従って、復号エラーが発生しても、暗号装置と復号装置との間で誤った鍵を共有することを防止できるという効果がある。

また、復号装置において、再度暗号文を生成する処理を行わないので、従来技術と比較すると、演算量を削減することができる。

これにより、ＮＴＲＵ暗号を用いて鍵カプセル化メカニズムを構成することができ、暗号装置と復号装置との間でＮＴＲＵ暗号を用いて鍵配送が行えるようになる。

また、本発明による方式は、非特許文献３に記述されている証明方法と同様の方法により、理論的にその安全性が証明できる。

４．７　変形例

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。以下のような場合も本発明に含まれる。

（１）用いるＮＴＲＵ暗号のパラメータＮ＝１６７に限定されない。パラメータＮは、他の値をとるとしてもよい。

（２）暗号化部１１４ｄ、第２関数部１１５ｄ、復号化部１２３ｄ及び第３関数部１２４ｄで行われるビット列と多項式との変換方法は、この方法に限られず他の変換方法でもよい。

例えば、ビット列と多項式を１対１に対応させる関数、又は関数値のテーブルを用いて変換してもよい。

また、例えば、実施の形態２の変形例（１）に述べた変換方法を用いて変換してもよい。

（３）暗号化部１１４ｄ及び復号化部１２３ｄで用いる公開鍵暗号方式は、暗号化部１１４ｄにおいて、検証値ａを公開鍵で暗号化して第１暗号文ｃ１を生成し、復号化部１２３ｄにおいて、第１暗号文ｃ１を秘密鍵で復号して、検証値ａと等しい復号検証値ａ’を生成できればよい。

従って、暗号化部１１４ｄ、復号化部１２３ｄで用いる公開鍵暗号は、ＮＴＲＵ暗号以外に、どんな公開鍵暗号でも利用できる。

例えば、ＲＳＡ暗号を採用するならば、ｈ、ｆをそれぞれＲＳＡ暗号の公開鍵、秘密鍵とし、暗号化部１１４ｄにおいて、ａをｈを用いて暗号化してｃ１を生成し、復号化部１２３ｄにおいて、ｃ１をｆを用いて復号してａ’を生成すればよい。

また、例えば、ＥｌＧａｍａｌ暗号採用するならば、ｈ，ｆをそれぞれＥｌＧａｍａｌ暗号の公開鍵，秘密鍵とし、暗号化部１１４ｄにおいて、乱数ｒを生成してａをｈとｒを用いて暗号化してｃ１を生成し、復号化部１２３ｄにおいて、ｃ１をｆを用いて復号してａ’を生成すればよい。

なお、ＲＳＡ暗号やＥｌＧａｍａｌ暗号について非特許文献１に詳細に記載されているため、ここでは説明を省略する。

（４）第１関数部１１３ｄは、関数値Ｇ（ｓ）の上位ｋビットを検証値ａをして下位ｋビットを共有鍵Ｋとする以外に、関数値Ｇ（ｓ）から検証値ａと共有鍵Ｋを導出すれば他の方法でもよい。

（５）第２関数部１１５ｄは、検証値ａと第１暗号文ｃ１から関数値Ｈ（ａ，ｃ１）を導出すれば他の方法でもよい。

例えば、任意の２項演算＃に対し、ａ＃ｃ１を関数Ｈに入力して関数値を導出してもよい。なお、ＮＴＲＵ暗号では第１暗号文ｃ１は多項式であるので、第１暗号文ｃ１から第１暗号文ビット列ｃ１’に変換し、ａ＃ｃ１’を関数Ｈに入力して関数値を導出してもよい。

（６）さらに、第２関数部１１５ｄは、検証値ａを用いて関数値を導出すれば、他の方法でもよい。

例えば、第２関数部１１５ｄは、Ｈ（ａ）を出力してもよいし、検証値ａをそのまま出力してもよい。すなわち、暗号装置１１０ｄにおいて、第２暗号文ｃ２を

・ｃ２＝ｓ　ｘｏｒ　Ｈ（ａ）、又は

・ｃ２＝ｓ　ｘｏｒ　ａとして導出してもよい。

これらの場合において、復号装置１２０ｄの第３関数部１２４ｄは、それぞれ、

・Ｈ（ａ’）　又は

・ａ’

を出力する。

（７）乱数マスク部１１６ｄは、乱数ｓと関数値Ｈ（ａ，ｃ１）とから第２暗号文ｃ２を導出し、乱数マスク除去部１２５ｄは、第２暗号文ｃ２と関数値Ｈ（ａ，ｃ１）とから乱数ｓが導出できれば、他の方法でもよい。

例えば、乱数マスク部１１６ｄは、第２暗号文ｃ２を

・ｃ２＝ｓ＋Ｈ（ａ，ｃ１）、又は

・ｃ２＝ｓ・Ｈ（ａ，ｃ１）

として導出してもよい。

５．実施の形態４

本発明に係るさらに別の実施の形態としてのコンテンツ配信システム１０ｅ（図示していない）について説明する。

コンテンツ配信システム１０ｅは、実施の形態３に示すコンテンツ配信システム１０ｄを基本として、これを変形したシステムであり、暗号装置が、関数値Ｇ（ｓ）から検証値ａと共有鍵Ｋの他に乱数値ｕを生成し、乱数値ｕを用いて検証値ａを暗号化して第１暗号文ｃ１を生成する点と、復号装置が、共有鍵Ｋを出力するときの判断の方法とにおいて、コンテン

ツ配信システム１０ｄと異なる。

ここでは、コンテンツ配信システム１０ｅについて、コンテンツ配信システム１０ｄとの差異点を中心に詳しく説明する。

５．１　コンテンツ配信システム１０ｅの構成

コンテンツ配信システム１０ｅは、コンテンツ配信システム１０ｄと同様の構成を有しており、暗号装置１１０ｄ及び復号装置１２０ｄに代えて、暗号装置１１０ｅ及び復号装置１２０ｅを含んでいる。その他の構成については、コンテンツ配信システム１０ｄにおけるものと同様であるので説明を省略する。

コンテンツ配信システム１０ｅは、ＮＴＲＵ暗号を用いて鍵配送を行うシステムである。暗号装置１１０ｅと復号装置１２０ｅとは、インターネット１３０を介して接続されている。

５．２　暗号装置１１０ｅの構成

暗号装置１１０ｅは、図１７に示すように、公開鍵入力部１１１ｄ、乱数生成部１１２ｄ、第１関数部１１３ｅ、暗号化部１１４ｅ、第２関数部１１５ｄ、乱数マスク部１１６ｄ、第１送信部１１７ｄ、共通鍵暗号部１１８及び第２送信部１１９から構成されている。

公開鍵入力部１１１ｄ、乱数生成部１１２ｄ、第２関数部１１５ｄ、乱数マスク部１１６ｄ、第１送信部１１７ｄ、共通鍵暗号部１１８及び第２送信部１１９は、暗号装置１１０ｄを構成する構成要素と同一であるので、説明を省略し、ここでは、暗号装置１１０ｄを構成する構成要素と異なる第１関数部１１３ｅ及び暗号化部１１４ｅについてその構成と動作を説明する。

（１）第１関数部１１３ｅ

第１関数部１１３ｅは、乱数生成部１１２ｄから乱数ｓを受け取り、受け取った乱数ｓの関数値Ｇ（ｓ）を生成する。次に、以下に示すようにして、生成した関数値Ｇ（ｓ）から検証値ａと共有鍵Ｋと乱数値ｕとを生成する。

ここで、関数Ｇは、出力長が３ｋビットのハッシュ関数であり、第１関数部１１３ｅは、Ｇ（ｓ）の上位ｋビットを検証値ａとし、Ｇ（ｓ）の中間のｋビットを共有鍵Ｋとし、Ｇ（ｓ）の下位ｋビットを乱数値ｕとする。

次に、第１関数部１１３ｅは、生成した検証値ａを暗号化部１１４ｅと第２関数部１１５ｄとへ出力し、生成した共有鍵Ｋを共通鍵暗号部１１８へ出力し、生成した乱数値ｕを暗号化部１１４ｅへ出力する。

（２）暗号化部１１４ｅ

暗号化部１１４ｅは、公開鍵入力部１１１ｄから公開鍵多項式ｈを受け取り、第１関数部１１３ｅから検証値ａと乱数値ｕとを受け取る。次に、以下に示すようにして、公開鍵多項式ｈと乱数値ｕとを用いて検証値ａの第１暗号文ｃ１を生成する。ここで、第１暗号文ｃ１は、ＮＴＲＵ暗号による暗号文である。また、乱数値ｕは、ブラインド値であり、暗号化の

対象である検証値ａを不明瞭にするために用いられる。

暗号化部１１４ｅは、ＮＴＲＵ暗号のパラメータｄに対し、ｄ個の項の各係数が「１」であり、他のｄ個の項の各係数が「－１」であり、残りの項の各係数が「０」となる乱数多項式ｒを乱数値ｕから一意に求まるように生成する。

具体的には、例えば、暗号化部１１４ｅは、乱数値ｕを擬似乱数系列の初期値（乱数シード）として設定し、{０，１，...，Ｎ－１}から重複しない２ｄ個の擬似乱数を生成し、最初のｄ個の擬似乱数により示される次元の項の係数を「１」とし、次のｄ個の擬似乱数により示される次元の項の係数を「－１」とし、残りの次元の項の係数を「０」とすることにより、乱数多項式ｒを生成する。

次に、暗号化部１１４ｅは、生成した乱数多項式ｒを用いて、暗号化部１１４ｄと同様にして、第１暗号文ｃ１＝Ｅ（ａｐ，ｒ，ｈ）を生成する。

次に、暗号化部１１４ｅは、生成した第１暗号文ｃ１を第２関数部１１５ｄと第１送信部１１７ｄとへ出力する。

５．３　復号装置１２０ｅの構成

復号装置１２０ｅは、図１８に示すように、秘密鍵入力部１２１ｅ、復号化部１２３ｅ、第３関数部１２４ｄ、乱数マスク除去部１２５ｄ、第４関数部１２６ｅ、比較部１２７ｅ、共通鍵復号部１２８及び第２受信部１２９から構成されている。

ここで、第３関数部１２４ｄ、乱数マスク除去部１２５ｄ、共通鍵復号部１２８及び第２受信部１２９については、復号装置１２０ｄに含まれている各構成要素と同一であるので、説明を省略し、復号装置１２０ｄに含まれている各構成要素と異なる秘密鍵入力部１２１ｅ、復号化部１２３ｅ、第４関数部１２６ｅ及び第２比較部１２７ｅについてその構成と動作を説明する。

（１）秘密鍵入力部１２１ｅ

秘密鍵入力部１２１ｅは、メモリカード１７０から復号装置１２０ｅの秘密鍵多項式ｆと公開鍵多項式ｈとを受け取り、秘密鍵多項式ｆを復号化部１２３ｅへ出力し、公開鍵多項式ｈを比較部１２７ｅへ出力する。

（２）復号化部１２３ｅ

復号化部１２３ｅは、秘密鍵入力部１２１ｅから秘密鍵多項式ｆを受け取り、第１受信部１２２ｄから第１暗号文ｃ１を受け取る。次に、秘密鍵多項式ｆを用いて、第１暗号文ｃ１を復号して復号検証値ａ’を生成し、生成した復号検証値ａ’を第３関数部１２４ｄへ出力し、受け取った第１暗号文ｃ１を比較部１２７ｅへ出力する。

（３）第４関数部１２６ｅ

第４関数部１２６ｅは、第１関数部１１３ｅが有する関数と同じ関数Ｇによるアルゴリズムを有している。

第４関数部１２６ｅは、乱数マスク除去部１２５ｄから復号乱数ｓ’を受け取り、受け取った復号乱数ｓ’のハッシュ関数値Ｇ（ｓ’）を生成する。次に、第１関数部１１３ｅと同様にして、関数値Ｇ（ｓ’）から検証値ａ’’と共有鍵Ｋ’と乱数値ｕ’とを生成し、検証値ａ’’と共有鍵Ｋ’と乱数値ｕ’とを比較部１２７ｅへ出力する。

（４）比較部１２７ｅ

比較部１２７ｅは、図１８に示すように、比較演算部１２７ｐ及び暗号化部１２７ｑから構成されている。

暗号化部１２７ｑは、秘密鍵入力部１２１ｅから公開鍵多項式ｈを受け取り、第４関数部１２６ｅから検証値ａ’’と乱数値ｕ’とを受け取る。次に、受け取った公開鍵多項式ｈと乱数値ｕ’とを用いて、暗号化部１１４ｄと同様にして、受け取った検証値ａ’’を暗号化して第１再暗号文ｃ１’を生成し、生成した第１再暗号文ｃ１’を比較演算部１２７ｐへ出力する。

比較演算部１２７ｐは、復号化部１２３ｂから第１暗号文ｃ１を受け取り、暗号化部１２７ｑから第１再暗号文ｃ１’を受け取る。次に、受け取った第１暗号文ｃ１と第１再暗号文ｃ１’とを比較して、ｃ１’＝ｃ１であるか否かを判断する。ｃ１’＝ｃ１であれば、受け取った共有鍵Ｋ’を共通鍵復号部１２８へ出力し、ｃ１’＝ｃ１でなければ、受け取った共有鍵Ｋ’を出力しない。

５．４　コンテンツ配信システム１０ｅの動作検証

以下に、コンテンツ配信システム１０ｅの全体の動作について、図１９に示す処理系統図を用いて説明する。

暗号装置１１０ｅは、復号装置１２０ｅの公開鍵多項式ｈを受け取り（ステップＳ２０１）、乱数ｓを生成し（ステップＳ２０２）、関数値Ｇ（ｓ）を生成し（ステップＳ２０３）、関数値Ｇ（ｓ）から検証値ａ、共有鍵Ｋ及び乱数値ｕを導出する（ステップＳ２０４ｅ）。次に、暗号装置１１０ｅは、検証値ａを、公開鍵多項式ｈ及び乱数値ｕを用いてＮＴＲＵ暗号で暗号化して第１暗号文ｃ１を生成し（ステップＳ２０５）、検証値ａと第１暗号文ｃ１から関数値Ｈ（ａ，ｃ１）を生成し（ステップＳ２０６）、乱数ｓと関数値Ｈ（ａ，ｃ１）から第２暗号文ｃ２＝ｓ　ｘｏｒ　Ｈ（ａ，ｃ１）を生成する（ステップＳ２０７）。次に、暗号装置１１０ｂは、第１暗号文ｃ１と第２暗号文ｃ２とをインターネット１３０を介して復号装置１２０ｅへ送信する（ステップＳ２０８）。

すなわち、この暗号装置１１０ｅは、以下の処理（ａ）～（ｄ）を行い、暗号文Ｃ＝（ｃ１，ｃ２）を復号装置１２０ｅへ送信する。

（ａ）乱数ｓを生成する。

（ｂ）Ｇ（ｓ）を生成し、Ｇ（ｓ）からａ，Ｋ，ｕを生成する。

（ｃ）公開鍵多項式ｈ，乱数値ｕを用いて検証値ａの第１暗号文ｃ１を生成する。

（d）ｃ２＝ｓ　ｘｏｒ　Ｈ（ａ，ｃ１）を生成する。

次に、暗号装置１１０ｅは、導出した共有鍵Ｋを用いて、コンテンツサーバ装置１４０から入力された平文ｍｉ（１≦ｉ≦ｎ）を共通鍵暗号で暗号化して暗号文Ｃｉ（１≦ｉ≦ｎ）を生成し（ステップＳ２０９）、インターネット１３０を介して復号装置１２０ｅへ送信する（ステップＳ２１０）。

一方、復号装置１２０ｅは、復号装置１２０ｅの秘密鍵多項式ｆ及び公開鍵多項式ｈを受け取り（ステップＳ２５１、ステップＳ２５１ｅ）、インターネット１３０を介して暗号装置１１０ｅから第１暗号文ｃ１と第２暗号文ｃ２を受信し（ステップＳ２０８）、第１暗号文ｃ１を秘密鍵多項式ｆを用いて復号して復号検証値ａ’を生成する（ステップＳ２５２）。次に、復号検証値ａ’と第１暗号文ｃ１から関数値Ｈ（ａ’，ｃ１）を生成し（ステップＳ２５３）、第２暗号文ｃ２と関数値Ｈ（ａ’，ｃ１）から復号乱数ｓ’＝ｃ２　ｘｏｒ　Ｈ（ａ’，ｃ１）を生成する（ステップＳ２５４）。次に、復号装置１２０ｅは、復号乱数ｓ’の関数値Ｇ（ｓ’）を生成し（ステップＳ２５５）、生成した関数値Ｇ（ｓ’）から検証値ａ’’、共有鍵Ｋ’及び乱数値ｕ’を導出する（ステップＳ２５６ｅ）。次に、検証値ａ’’を暗号化して第１再暗号文ｃ１’を生成し（ステップＳ２６１）、ｃ１’＝ｃ１であれば（ステップＳ２５７ｅ）、共有鍵Ｋ’を出力する（ステップＳ２５８）。

すなわち、復号装置１２０ｅは、以下の処理（ａ）～（ｅ）を行い、共有鍵Ｋ’を導出する。

（ａ）秘密鍵多項式ｆを用いて第１暗号文ｃ１を復号してａ’を生成する。

（ｂ）ｓ’＝ｃ２　ｘｏｒ　Ｈ（ａ’，ｃ１）を生成する。

（ｃ）Ｇ（ｓ’）を生成し、Ｇ（ｓ’）からａ’’，Ｋ’，ｕ’を生成する。

（ｄ）公開鍵多項式ｈ及び乱数値ｕ’を用いてａ’’の第１再暗号文ｃ１’を生成する。

（ｅ）ｃ１’＝ｃ１が成立するかどうかチェックする。成立すれば共有鍵Ｋ’を出力する。

ここで、暗号装置１１０ｅで用いられた公開鍵多項式ｈに対応する正しい秘密鍵多項式ｆが復号装置１２０ｅで用いられれば、第１暗号文ｃ１は正しく復号されて、復号検証値ａ’＝ａとなり、第２暗号文ｃ２とＨ（ａ’，ｃ１）から生成される復号乱数ｓ’＝ｓとなる。従って、Ｇ（ｓ’）から導出される検証値ａ’’＝ａとなり、共有鍵Ｋ’＝Ｋとなり、乱数値ｕ’＝ｕとなる。そして、ａ’’＝ａ及びｕ’＝ｕが成り立つので、ｃ１’＝ｃ１が成り立ち、復号装置１２０ｅは暗号装置１１０ｅと同じ共有鍵Ｋを導出できることになる。

次に、復号装置１２０ｅは、導出した共有鍵Ｋ’（＝Ｋ）を用いて、インターネット１３０を介して暗号装置１１０ｅから共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を受信し（ステップＳ２１０）、受信した共通鍵暗号文Ｃｉ（１≦ｉ≦ｎ）を共通鍵暗号で復号して復号文ｍｉ’（１≦ｉ≦ｎ）を生成し（ステップＳ２５９）、生成した復号文ｍｉ’（１≦ｉ≦ｎ）を再生装置１５０へ出力する。

ここで、共通鍵暗号文生成時に用いた暗号鍵Ｋと復号文生成時に用いる暗号鍵Ｋ’とは同一であるので、復号装置１２０ｅは、正しくｍｉ’＝ｍｉ（１≦ｉ≦ｎ）を得ることができる。

５．５　コンテンツ配信システム１０ｅにおける効果

従来のＰＳＥＣ－ＫＥＭアルゴリズムでは、ハッシュ関数Ｈの入力にａ＊Ｐ、ａ＊Ｗを用い、秘密鍵を用いずにａ＊Ｐからａ＊Ｗを計算することが困難なＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題を用いて、最終的に共有鍵Ｋを導出することにより、秘密鍵を知らなければその共有鍵Ｋを導出できないようにしている。従って、ＮＴＲＵ暗号をはじめ、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題を利用しない他の公開鍵暗号では、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題のａ＊Ｐ、ａ＊Ｗに相当するものがないため、ＰＳＥＣ－ＫＥＭアルゴリズムを適用できないという問題点がある。

しかしながら、本発明のコンテンツ配信システム、暗号装置及び復号装置では、ハッシュ関数Ｈの入力を検証値ａとその暗号文ｃ１としたので、実施の形態３と同様に、ＮＴＲＵ暗号や他の公開鍵暗号を適用できる。

なお、復号エラーが発生すると、復号装置は誤った復号検証値ａ’を得ることになるが、ｃ１’はｃ１と等しくならないために、共有鍵Ｋ’を出力しない。従って、復号エラーが発生しても、暗号装置と復号装置との間で誤った鍵を共有することを防止できるという効果もある。

これにより、ＮＴＲＵ暗号を用いて鍵カプセル化メカニズムを構成することができ、暗号装置と復号装置との間でＮＴＲＵ暗号を用いて鍵配送が行えるようになる。

また、本発明による方式は、非特許文献３に記述されている証明方法と同様の方法により、理論的にその安全性が証明できる。

５．６　変形例

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その主旨を逸脱しない範囲において種々なる態様で実施し得るものである。実施の形態３におけるのと同様の変形を施すことができるのはもちろんであるが、以下のような場合も本発明に含まれる。

（１）暗号化部１１４ｅで行われる乱数値ｕから乱数多項式ｒへの変換方法は、この方法に限られずｕからｒが一意に求まれば他の変換方法でもよい。例えば、乱数値ｕを多項式に対応させる関数、又は関数値テーブルを用いて変換してもよい。

また、例えば、実施の形態２の変形例（１）に述べた変換方法を用いて変換してもよい。

（２）暗号化部１１４ｅ及び復号化部１２３ｅで用いる公開鍵暗号は、暗号化部１１４ｅにおいて、検証値ａを公開鍵と乱数値ｕとを用いて暗号化して第１暗号文ｃ１を生成し、復号化部１２３ｅにおいて、第１暗号文ｃ１を秘密鍵で復号して、検証値ａと等しい復号検証

値ａ’を生成できればよい。従って、暗号化部１１４ｅ及び復号化部１２３ｅで用いる公開鍵暗号は、ＮＴＲＵ暗号以外に、乱数を用いる公開鍵暗号ならばどんな暗号でも利用できる。

例えば、ＥｌＧａｍａｌ暗号ならば、ｈ、ｆをそれぞれＥｌＧａｍａｌ暗号の公開鍵、秘密鍵とし、暗号化部１１４ｅにおいて、ａをｈと乱数値ｕとを用いて暗号化してｃ１を生成し、復号化部１２３ｅにおいて、ｃ１をｆを用いて復号してａ’を生成すればよい。

（３）乱数値ｕは、第１関数部１１３ｅ及び第４関数部１２６ｅで生成される以外にも、暗号装置１１０ｅと復号装置１２０ｅとで同じ値を得られれば、他の生成方法でもよい。

例えば、任意の関数Ｆｕｎｃに対し、ｕ＝Ｆｕｎｃ（ｓ）として暗号装置１１０ｅと復号装置１２０ｅとで同じ値を得られるようにしてもよい。すなわち、

・Ｇ（ｓ）を生成し、Ｇ（ｓ）からａ、Ｋを生成する。

・Ｆｕｎｃ（ｓ）を生成し、ｕ＝Ｆｕｎｃ（ｓ）とする。

としてもよい。

（４）さらに、乱数値ｕは、第１関数部１１３ｅ及び第４関数部１２６ｅで生成される以外にも、暗号装置１１０ｅと復号装置１２０ｅとで同じ値を得られればよいため、暗号装置１１０ｅが乱数値ｕを復号装置１２０ｅに直接送信してもよい。

すなわち、以下のように、暗号文Ｃと乱数値ｕとを復号装置１２０ｅに送信してもよい。

・Ｇ（ｓ）を生成し、Ｇ（ｓ）からａ、Ｋを生成する。

・暗号装置１１０ｅは、別途、乱数値ｕを、復号装置１２０ｅへ送信する。

また、暗号装置１１０ｅは、乱数値ｕを暗号化して送信してもよい。

（５）さらに、乱数値ｕは、暗号装置１１０ｅと復号装置１２０ｅとで同じ値を得られればよいため、乱数値ｕの一部から構成される部分情報を第１関数部１１３ｅ及び第４関数部１２６ｅで生成し、乱数値ｕの残りの部分情報を暗号装置１１０ｅから復号装置１２０ｅに直接送信してもよい。

例えば、以下のように、暗号文Ｃと乱数値ｕ２とを復号装置１２０ｅに送信してもよい。

・Ｇ（ｓ）を生成し、Ｇ（ｓ）からａ、Ｋ、ｕ１を生成する。

・暗号装置１１０ｅは、別途、乱数値ｕ２を、復号装置１２０ｅへ送信する。

・乱数値ｕを、ｕ＝ｕ１　ｘｏｒ　ｕ２により生成する。

また、暗号装置１１０ｅは、乱数値ｕ２を暗号化して送信してもよい。

（６）復号装置１２０ｅは、第１暗号文ｃ１が第４関数部１２６ｅで得られる検証値ａ’’の暗号文かどうかチェックを行い、ｃ１がａ’’の暗号文であるときに共有鍵Ｋ’を用いて共通鍵暗号文Ｃｉを復号しているが、実施の形態３の復号装置１２０ｄと同じチェック方法により行うとしてもよい。

すなわち、図２０の処理系統図に示すように、復号装置１２０ｄと同じ復号化部１２３ｄ及び比較部１２７ｄを用いて、以下のように、チェックしてもよい。

（a）秘密鍵多項式ｆを用いて第１暗号文ｃ１を復号してａ’を生成する（ステップＳ２５２）。

（b）ｓ’＝ｃ２　ｘｏｒ　Ｈ（ａ’，ｃ１）を生成する（ステップＳ２５４）。

（c）Ｇ（ｓ’）を生成し（ステップＳ２５５）、Ｇ（ｓ’）からａ’’、Ｋ’、ｕ’を生成する（ステップＳ２５６ｅ）。

（d）ａ’’＝ａ’が成立するかどうかチェックする（ステップＳ２５７）。成立すれば共有鍵Ｋ’を出力する（ステップＳ２５８）。

また、このチェックは、第１暗号文ｃ１が復号検証値ａ’の暗号文かどうかのチェックでもよい。

７．実施の形態３及び実施の形態４のまとめ

以上説明したように、本発明は、共有鍵データと、予め与えられた公開鍵データに基づいて前記共有鍵データを暗号化した暗号化共有鍵データを出力する共有鍵生成装置であって、秘密数データを生成する秘密数データ生成部と、前記秘密数データを所定の処理に基づいて検証値データと前記共有鍵データに変換する共有鍵導出部と、前記検証値データを前記公開鍵データに基づいて暗号化して第１の暗号予備データを生成する第１の暗号化部と、前記検証値データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記秘密数データを前記変換検証値データに基づいて暗号化して第２の暗号予備データを生成する第２の暗号化部とを備え、前記暗号化共有鍵データは、前記第１の暗号予備データと前記第２の暗号予備データから構成される。

また、本発明は、共有鍵データと、予め与えられた公開鍵データに基づいて前記共有鍵データを暗号化した暗号化共有鍵データを出力する共有鍵生成装置であって、秘密数データを生成する秘密数データ生成部と、前記秘密数データと前記第１の暗号予備データを所定の処理に基づいて検証値データと前記共有鍵データに変換する共有鍵導出部と、前記検証値データを前記公開鍵データに基づいて暗号化して第１の暗号予備データを生成する第１の暗号化部と、前記検証値データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記秘密数データを前記変換検証値データに基づいて暗号化して第２の暗号予備データを生成する第２の暗号化部とを備え、前記暗号化共有鍵データは、前記第１の暗号予備データと前記第２の暗号予備データから構成される。

また、本発明は、共有鍵データと、予め与えられた公開鍵データに基づいて前記共有鍵データを暗号化した暗号化共有鍵データを出力する共有鍵生成装置であって、秘密数データを生成する秘密数データ生成部と、前記秘密数データを所定の処理に基づいて検証値データと乱数データと前記共有鍵データとに変換する共有鍵導出部と、前記検証値データを前記公開鍵データと前記乱数データに基づいて暗号化して第１の暗号予備データを生成する第１の暗号化部と、前記検証値データを所定の処理に基づいて変換検証値データに変換する検証値変

換部と、前記秘密数データを前記変換検証値データに基づいて暗号化して第２の暗号予備データを生成する第２の暗号化部とを備え、前記暗号化共有鍵データは、前記第１の暗号予備データと前記第２の暗号予備データから構成される。

また、本発明は、共有鍵データと、予め与えられた公開鍵データに基づいて前記共有鍵データを暗号化した暗号化共有鍵データを出力する共有鍵生成装置であって、秘密数データを生成する秘密数データ生成部と、前記秘密数データを所定の処理に基づいて検証値データと乱数データと前記共有鍵データとに変換する共有鍵導出部と、前記検証値データを前記公開鍵データと前記乱数データに基づいて暗号化して第１の暗号予備データを生成する第１の暗号化部と、前記検証値データと前記第１の暗号予備データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記秘密数データを前記変換検証値データに基づいて暗号化して第２の暗号予備データを生成する第２の暗号化部とを備え、前記暗号化共有鍵データは、前記第１の暗号予備データと前記第２の暗号予備データから構成される。

ここで、前記秘密数データは、ランダムに生成される乱数であるとしてもよい。

ここで、前記共有鍵導出部は、所定の処理として、一方向性ハッシュ関数を用いるとしてもよい。

ここで、前記第１の暗号化部は、ＮＴＲＵ暗号方式により暗号化して前記第１の暗号予備データを生成するとしてもよい。

ここで、前記検証値変換部は、所定の処理として、一方向性ハッシュ関数を用いるとしてもよい。

ここで、前記検証値変換部は、所定の処理として、前記検証値データをそのまま前記変換検証値データとするとしてもよい。

ここで、前記第２の暗号化部は、前記秘密数データと前記変換検証値データの排他的論理和演算を行って前記第２の暗号予備データを生成するとしてもよい。

ここで、前記第２の暗号化部は、前記秘密数データを、前記変換検証値データを暗号鍵として用いて共通鍵暗号方式により暗号化して前記第２の暗号予備データを生成するとしてもよい。

ここで、前記第２の暗号化部は、前記秘密数データに前記変換検証値データを加算して前記第２の暗号予備データを生成するとしてもよい。

ここで、前記第２の暗号化部は、前記秘密数データに前記変換検証値データを乗算して前記第２の暗号予備データを生成するとしてもよい。

ここで、前記暗号化共有鍵データは、前記第１の暗号予備データと前記第２暗号予備データのビット連結データであるとしてもよい。

また、本発明は、予め与えられた秘密鍵データに基づいて、第１の暗号予備データと第２の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力すると

有鍵復元装置であって、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第１の復号化部と、前記検証値データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記第２の暗号予備データを前記変換検証値データに基づいて復号化して秘密数データを生成する第２の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと前記共有鍵データに変換する共有鍵導出部とを備え、前記検証値データと前記検証値検証データが一致する場合に、前記共有鍵データを出力する。

また、本発明は、予め与えられた秘密鍵データに基づいて、第１の暗号予備データと第２の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第１の復号化部と、前記検証値データと前記第１の暗号予備データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記第２の暗号予備データを前記変換検証値データに基づいて復号化して秘密数データを生成する第２の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと前記共有鍵データに変換する共有鍵導出部とを備え、前記検証値データと前記検証値検証データが一致する場合に、前記共有鍵データを出力する。

また、本発明は、予め与えられた秘密鍵データに基づいて、第１の暗号予備データと第２の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第１の復号化部と、前記検証値データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記第２の暗号予備データを前記変換検証値データに基づいて復号化して秘密数データを生成する第２の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出部とを備え、前記検証値データと前記検証値検証データが一致する場合に、前記共有鍵データを出力する。

また、本発明は、予め与えられた秘密鍵データに基づいて、第１の暗号予備データと第２の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第１の復号化部と、前記検証値データと前記第１の暗号予備データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記第２の暗号予備データを前記変換検証値データに基づいて復号化して秘密数データを生成する第２の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出部とを備え、前記検証値データと前記検証値検証データが一致する場合に、前記共有鍵データを出力する。

また、本発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、第１の暗号予備データと第２の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第１の復号化部と、前記検証値データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記第２の暗号予備データを前記変換検証値データに基づいて復号化して秘密数データを生成する第２の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出部と、前記検証値検証データを前記公開鍵データと前記乱数データに基づいて暗号化して第３の暗号予備データを生成する第３の暗号化部とを備え、前記第１の暗号予備データと前記第３の暗号予備データが一致する場合に、前記共有鍵データを出力する。

また、本発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、第１の暗号予備データと第２の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第１の復号化部と、前記検証値データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記第２の暗号予備データを前記変換検証値データに基づいて復号化して秘密数データを生成する第２の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出部と、前記検証値データを前記公開鍵データと前記乱数データに基づいて暗号化して第３の暗号予備データを生成する第３の暗号化部とを備え、前記第１の暗号予備データと前記第３の暗号予備データが一致する場合に、前記共有鍵データを出力する。

また、本発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、第１の暗号予備データと第２の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第１の復号化部と、前記検証値データと前記第１の暗号予備データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記第２の暗号予備データを前記変換検証値データに基づいて復号化して秘密数データを生成する第２の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出部と、前記検証値検証データを前記公開鍵データと前記乱数データに基づいて暗号化して第３の暗号予備データを生成する第３の暗号化部とを備え、前記第１の暗号予備データと前記第３の暗号予備データが一致する場合に、前記共有鍵データを出力する。

また、本発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、第１の暗号予備データと第２の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵デ

ータを出力する共有鍵復元装置であって、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第１の復号化部と、前記検証値データと前記第１の暗号予備データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記第２の暗号予備データを前記変換検証値データに基づいて復号化して秘密数データを生成する第２の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出部と、前記検証値データを前記公開鍵データと前記乱数データに基づいて暗号化して第３の暗号予備データを生成する第３の暗号化部とを備え、前記第１の暗号予備データと前記第３の暗号予備データが一致する場合に、前記共有鍵データを出力する。

ここで、前記共有鍵導出部は、所定の処理として、一方向性ハッシュ関数を用いるとしてもよい。

ここで、前記第１の復号化部は、ＮＴＲＵ暗号方式により復号化して検証値データを生成するとしてもよい。

ここで、前記検証値変換部は、所定の処理として、一方向性ハッシュ関数を用いるとしてもよい。

ここで、前記検証値変換部は、所定の処理として、前記検証値データをそのまま前記変換検証値データとするとしてもよい。

ここで、前記第２の復号化部は、前記第２の暗号予備データと前記変換検証値データの排他的論理和演算を行って前記秘密数データを生成するとしてもよい。

ここで、前記第２の復号化部は、前記第２の暗号予備データを、前記変換検証値データを暗号鍵として用いて共通鍵暗号方式により復号化して前記秘密数データを生成するとしてもよい。

ここで、前記第２の復号化部は、前記第２の暗号予備データに前記変換検証値データを減算して前記秘密数データを生成するとしてもよい。

ここで、前記第２の暗号化部は、前記第２の暗号予備データを前記変換検証値データで除算して前記秘密数データを生成するとしてもよい。

また、本発明は、予め与えられた公開鍵データに基づいて平文データを暗号化した暗号文データを生成する暗号装置であって、秘密数データを生成する秘密数データ生成部と、前記秘密数データを所定の処理に基づいて検証値データと共有鍵データに変換する共有鍵導出部と、前記検証値データを前記公開鍵データに基づいて暗号化して第１の暗号予備データを生成する第１の暗号化部と、前記検証値データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記秘密数データを前記変換検証値データに基づいて暗号化して第２の暗号予備データを生成する第２の暗号化部と、前記平文データを前記共有鍵データに基づいて暗号化して第３の暗号予備データを生成する第３の暗号化部とを備え、前記暗号文デ

ータは、前記第１の暗号予備データと前記第２の暗号予備データと前記第３の暗号予備データから構成される。

また、本発明は、予め与えられた秘密鍵データに基づいて、第１の暗号予備データと第２の暗号予備データと第３の暗号予備データから構成される暗号文データを復号して復号文データを出力する復号装置であって、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第１の復号化部と、前記検証値データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記第２の暗号予備データを前記変換検証値データに基づいて復号化して秘密数データを生成する第２の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと共有鍵データに変換する共有鍵導出部とを備え、前記検証値データと前記検証値検証データが一致する場合に、前記第３の暗号予備データを前記共有鍵データに基づいて復号化して前記復号文データを生成する復号部とを備える。

また、本発明は、予め与えられた公開鍵データに基づいて平文データを暗号化した暗号文データを生成する暗号装置、及び予め与えられた秘密鍵データに基づいて暗号文データを復号して復号文データを出力する復号装置からなる暗号システムである。前記暗号装置は、秘密数データを生成する秘密数データ生成部と、前記秘密数データを所定の処理に基づいて検証値データと共有鍵データに変換する共有鍵導出部と、前記検証値データを前記公開鍵データに基づいて暗号化して第１の暗号予備データを生成する第１の暗号化部と、前記検証値データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記秘密数データを前記変換検証値データに基づいて暗号化して第２の暗号予備データを生成する第２の暗号化部と、前記平文データを前記共有鍵データに基づいて暗号化して第３の暗号予備データを生成する第３の暗号化部とを備え、前記暗号文データは、前記第１の暗号予備データと前記第２の暗号予備データと前記第３の暗号予備データから構成される。前記復号装置は、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して前記検証値データを生成する第１の復号化部と、前記検証値データを所定の処理に基づいて前記変換検証値データに変換する検証値変換部と、前記第２の暗号予備データを前記変換検証値データに基づいて復号化して前記秘密数データを生成する第２の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと共有鍵データに変換する共有鍵導出部とを備え、前記検証値データと前記検証値検証データが一致する場合に、前記第３の暗号予備データを前記共有鍵データに基づいて復号化して前記復号文データを生成する復号部とを備える。

以上に説明したように、本発明は、従来システムにおける問題点を鑑みて行われたもので、暗号システムにおいて、ＮＴＲＵ暗号を適用できる鍵カプセル化メカニズムを構成することで、暗号装置と復号装置との間でＮＴＲＵ暗号を用いて鍵配送が行えるようになる。

以上により、従来技術では達成できなかった暗号システムを提供することができ、その価

値は大きい。

８．その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

（１）暗号装置が、インターネットを介して、各暗号文を復号装置へ送信する代わりに、暗号装置は、各暗号文をＤＶＤなどの記録媒体に書き込み、復号装置は、記録媒体から各暗号文を読み出すとしてもよい。

（２）本発明で用いるＮＴＲＵ暗号は、非特許文献２に記載の方式以外に、ＥＥＳＳ（Efficient Embedded Security Standard）方式のＮＴＲＵ暗号であってもよい。ＥＥＳＳ方式のＮＴＲＵ暗号については、"EESS;Consortium for Efficient Embedded Security, Efficient Embedded Security Standards #1:Implementation Aspects of NTRU Encrypt and NTRU Sign, Version 2.0 ," available at http://ceesstandards.org , May 2003.に詳細に記述されている。このため、ここではその詳細については説明を省くが、以下に簡単に説明する。

ＥＥＳＳ方式のＮＴＲＵ暗号では、乱数多項式ｒは、ｄ個の係数が１であり、（Ｎ－ｄ）個の係数が０である多項式、もしくはこのような複数の多項式を用いて計算される多項式である。従って、上記の実施の形態において、乱数多項式ｒを生成する際に、このような多項式となるように生成すれば、ＮＴＲＵ暗号の代わりにＥＥＳＳ方式のＮＴＲＵ暗号を用いることができ、同様の効果が得られる。

（３）コンテンツ配信システムは、次に示すように構成してもよい。

コンテンツ配信システムは、コンテンツサーバ装置と暗号装置と放送装置と受信装置と復号装置と再生装置とモニタとから構成されている。

暗号装置と復号装置とは、コンテンツ配信システム１０の暗号装置１１０と復号装置１２０とに対応している。

コンテンツサーバ装置と暗号装置とは、専用回線を介して接続されており、コンテンツサーバ装置は、映像と音声から構成される映画などのコンテンツを専用回線を介して暗号装置へ送信する。暗号装置と放送装置とは、専用回線を介して接続されている。暗号装置は、各暗号文を放送装置へ送信し、放送装置は、各暗号文を多重化し、デジタル放送波に乗せて放送する。

受信装置と復号装置とは、接続されており、復号装置と再生装置とは、接続されている。受信装置は、デジタル放送波を受信し、受信したデジタル放送波から各暗号文を抽出し、抽出した各暗号文を復号装置へ送信する。復号装置は、各暗号文を受け取り、受け取った各暗号文を用いて、再生コンテンツを生成し、生成した再生コンテンツを再生装置へ出力する。再生装置は、復号装置及びスピーカを内蔵するモニタに接続されている。再生装置は、再生

コンテンツを受け取り、受け取った再生コンテンツから映像信号及び音声信号を生成し、モニタは、映像を表示し、音声を出力する。

（4）コンテンツサーバ装置と暗号装置とは、一体となった装置から構成されているとしてもよい。また、復号装置と再生装置とは、一体となった装置から構成されているとしてもよい。

（5）上記の各実施の形態において、メモリカード１６０は、予め公開鍵多項式ｈを記憶しており、メモリカード１７０は、予め秘密鍵多項式ｆ及び公開鍵多項式ｈを記憶しており、暗号装置１１０及び復号装置１２０は、メモリカード１６０及びメモリカード１７０から、それぞれ公開鍵多項式、秘密鍵多項式を取得するとしているが、これには限定されない。

暗号装置１１０は、予め公開鍵多項式を記憶しており、復号装置１２０は、予め公開鍵多項式及び秘密鍵多項式を記憶しているとしてもよい。

また、鍵管理装置は、秘密鍵多項式及び公開鍵多項式を生成し、生成した秘密鍵多項式及び公開鍵多項式を秘密にかつ安全に復号装置１２０へ送信し、生成した公開鍵多項式を暗号装置１１０へ送信するとしてもよい。

（6）コンテンツ配信システムにおいて配信されるコンテンツは、映像と音声とからなる映画などのコンテンツには、限定されない。動画像、静止画像、音声、音楽、文書、小説、ＤＢソフトにより生成されるデータベース、表計算ソフトにより生成される電子的な表データ、コンピュータプログラム、その他コンピュータ用データなどあってもよい。

また、前記コンテンツは、上記のような著作物ではなく、暗号化及び復号化、デジタル署名及び署名検証などに用いる鍵情報であるとしてもよい。

例えば、上記の各実施の形態により示されるようにして、暗号装置及び復号装置は、共有鍵を共有し、暗号装置は、コンテンツ鍵を共有鍵を用いて暗号化して暗号化コンテンツ鍵を生成し、コンテンツをコンテンツ鍵を用いて暗号化して暗号化コンテンツを生成し、生成した暗号化コンテンツ鍵と生成した暗号化コンテンツとを復号装置に送信する。復号装置は、暗号化コンテンツ鍵と暗号化コンテンツとを受信し、共有鍵を用いて、暗号化コンテンツ鍵を復号してコンテンツ鍵を生成し、生成したコンテンツ鍵を用いて暗号化コンテンツを復号してコンテンツを生成するとしてもよい。

（7）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ―ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ　Ｄｉｓｃ）、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記

コンピュータプログラム又は前記デジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

（8）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

Although the present invention has been fully described by way of examples with reference to the accompanying drawings,it is to be noted that various changes and modifications will be apparent to those skilled in the art. Therefore, unless otherwise such changes and modifications depart from the scope of the present invention, they should be construed as being included therein.

産業上の利用の可能性

上記において説明したコンテンツ配布システムは、コンテンツ供給者から利用者に対して、音楽、映画、小説などのデジタル化された著作物を供給する産業において、経営的、反復的かつ継続的に使用される。また、コンテンツ配布システムを構成する暗号装置及び復号装置は、電化製品などを製造する電機機器産業において、製造され、販売される。

特に、デシタル化された著作物を、ＤＶＤなどの記録媒体に格納して市場に流通させることにより、ネットワークを介して流通させることにより、又は放送により、供給する産業において好適である。

【What is claimed is:】

1．第３者に知られることなく共有鍵を生成する共有鍵生成装置及び共有鍵復元装置から構成される鍵共有システムであって、

前記共有鍵生成装置は、

シード値を生成するシード値生成手段と、

生成された前記シード値から検証値及び共有鍵を生成する第１共有鍵生成手段と、

生成された前記検証値を暗号化して、第１暗号化情報を生成する第１暗号化手段と、

生成された前記検証値に基づいて、生成された前記シード値を暗号化して、第２暗号化情報を生成する第２暗号化手段と、

生成された前記第１暗号化情報及び前記第２暗号化情報を送信する送信手段とを備え、

前記共有鍵復元装置は、

前記第１暗号化情報及び前記第２暗号化情報を受信する受信手段と、

受信された前記第１暗号化情報を復号して第１復号検証値を生成する第１復号手段と、

生成された前記第１復号検証値に基づいて、受信された前記第２暗号化情報を復号して、復号シード値を生成する第２復号手段と、

前記第１共有鍵生成手段と同一の方法により、生成された前記復号シード値から第２復号検証値及び復号共有鍵を生成する第２共有鍵生成手段と、

生成された前記第１復号検証値及び前記第２復号検証値に基づいて、生成された前記復号共有鍵を出力するか否かを判断する判断手段と、

出力すると判断される場合に、生成された前記復号共有鍵を出力する出力手段とを備える

ことを特徴とする鍵共有システム。

2．前記共有鍵生成装置は、さらに、

コンテンツを取得する取得手段と、

生成された前記共有鍵を用いて、取得されたコンテンツを暗号化して、暗号化コンテンツを生成する暗号化手段とを備え、

前記送信手段は、さらに、生成された前記暗号化コンテンツを送信し、

前記受信手段は、さらに、前記暗号化コンテンツを受信し、

前記共有鍵復元装置は、さらに、

出力された前記復号共有鍵を用いて、受信された前記暗号化コンテンツを復号して、復号コンテンツを生成する復号手段と、

生成された復号コンテンツを出力する出力手段とを備える

ことを特徴とする請求の範囲１に記載の鍵共有システム。

3．第３者に知られることなく共有鍵を相手の装置へ伝える共有鍵生成装置であって、

シード値を生成するシード値生成手段と、

生成された前記シード値から検証値及び共有鍵を生成する共有鍵生成手段と、

生成された前記検証値を暗号化して、第１暗号化情報を生成する第１暗号化手段と、

生成された前記検証値に基づいて、生成された前記シード値を暗号化して、第２暗号化情報を生成する第２暗号化手段と、

生成された前記第１暗号化情報及び前記第２暗号化情報を送信する送信手段と

を備えることを特徴とする共有鍵生成装置。

４．前記シード値生成手段は、乱数を生成し、生成した乱数を前記シード値とすることにより、前記シード値を生成する

ことを特徴とする請求の範囲３に記載の共有鍵生成装置。

５．前記共有鍵生成手段は、前記シード値に一方向性関数を施して関数値を生成し、生成した前記関数値から前記検証値及び前記共有鍵を生成する

ことを特徴とする請求の範囲３に記載の共有鍵生成装置。

６．前記共有鍵生成手段は、前記シード値に、前記一方向性関数として、ハッシュ関数を施して前記関数値を生成する

ことを特徴とする請求の範囲５に記載の共有鍵生成装置。

７．前記共有鍵生成手段は、生成された前記関数値の一部を前記検証値とし、他の一部を前記共有鍵とすることにより、前記検証値及び前記共有鍵を生成する

ことを特徴とする請求の範囲５に記載の共有鍵生成装置。

８．前記共有鍵生成手段は、前記シード値に一方向性関数を施して関数値を生成し、生成した前記関数値から前記検証値、前記共有鍵及びブラインド値を生成する

ことを特徴とする請求の範囲３に記載の共有鍵生成装置。

９．前記第１暗号化手段は、

公開鍵を取得する公開鍵取得部と、

取得された前記公開鍵及び生成された前記ブラインド値を用いて、前記検証値に公開鍵暗号化アルゴリズムを施して前記第１暗号化情報を生成する公開鍵暗号化部と含む

ことを特徴とする請求の範囲８に記載の共有鍵生成装置。

10．前記公開鍵暗号化アルゴリズムは、ＮＴＲＵ暗号方式によるものであり、

前記公開鍵取得部は、前記公開鍵として、ＮＴＲＵ暗号方式の鍵生成アルゴリズムにより生成された公開鍵多項式を取得し

前記公開鍵暗号化部は、前記検証値から検証値多項式を生成し、前記ブラインド値からブラインド値多項式を生成し、ＮＴＲＵ暗号方式の暗号化アルゴリズムにより、前記公開鍵多項式を鍵として用い、前記検証値多項式を攪乱するために前記ブラインド値多項式を用いて、前記検証値多項式を暗号化して、多項式としての前記第１暗号化情報を生成する

ことを特徴とする請求の範囲９に記載の共有鍵生成装置。

11. 前記第１暗号化手段は、

公開鍵を取得する公開鍵取得部と、

取得された前記公開鍵を用いて、前記検証値に公開鍵暗号化アルゴリズムを施して前記第１暗号化情報を生成する公開鍵暗号化部と含む

ことを特徴とする請求の範囲３に記載の共有鍵生成装置。

12. 前記公開鍵暗号化アルゴリズムは、ＮＴＲＵ暗号方式によるものであり、

前記公開鍵取得部は、前記公開鍵として、ＮＴＲＵ暗号方式の鍵生成アルゴリズムにより生成された公開鍵多項式を取得し

前記公開鍵暗号化部は、前記検証値から検証値多項式を生成し、ブラインド値を生成し、生成した前記ブラインド値からブラインド値多項式を生成し、ＮＴＲＵ暗号方式の暗号化アルゴリズムにより、前記公開鍵多項式を鍵として用い、前記検証値多項式を攪乱するために前記ブラインド値多項式を用いて、前記検証値多項式を暗号化して、多項式としての前記第１暗号化情報を生成する

ことを特徴とする請求の範囲１１に記載の共有鍵生成装置。

13. 前記第２暗号化手段は、前記検証値に一方向性関数を施して関数値を生成し、生成した前記関数値を用いて、前記シード値に暗号化アルゴリズムを施して前記第２暗号化情報を生成する

ことを特徴とする請求の範囲３に記載の共有鍵生成装置。

14. 前記第２暗号化手段は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして排他的論理和を施すことにより、前記第２暗号化情報を生成する

ことを特徴とする請求の範囲１３に記載の共有鍵生成装置。

15. 前記第２暗号化手段は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして共通鍵暗号化アルゴリズムを施すことにより、前記第２暗号化情報を生成する

ことを特徴とする請求の範囲１３に記載の共有鍵生成装置。

16. 前記第２暗号化手段は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして加算を施すことにより、前記第２暗号化情報を生成する

ことを特徴とする請求の範囲１３に記載の共有鍵生成装置。

17. 前記第２暗号化手段は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして乗算を施すことにより、前記第２暗号化情報を生成する

ことを特徴とする請求の範囲１３に記載の共有鍵生成装置。

18. 前記第２暗号化手段は、前記検証値に、前記一方向性関数としてハッシュ関数を施して前記関数値を生成する

ことを特徴とする請求の範囲１３に記載の共有鍵生成装置。

19. 前記第２暗号化手段は、前記検証値を用いて、前記シード値に暗号化アルゴリズムを施

して第２暗号化情報を生成する

ことを特徴とする請求の範囲３に記載の共有鍵生成装置。

20. 前記第２暗号化手段は、前記検証値及び前記第１暗号化情報を用いて、前記シード値を暗号化する

ことを特徴とする請求の範囲３に記載の共有鍵生成装置。

21. 前記第２暗号化手段は、前記検証値及び前記第１暗号化情報に一方向性関数を施して関数値を生成し、生成した前記関数値を用いて、前記シード値に暗号化アルゴリズムを施して前記第２暗号化情報を生成する

ことを特徴とする請求の範囲２０に記載の共有鍵生成装置。

22. 前記第２暗号化手段は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして排他的論理和を施すことにより、前記第２暗号化情報を生成する

ことを特徴とする請求の範囲２１に記載の共有鍵生成装置。

23. 前記共有鍵生成装置は、さらに、

コンテンツを取得する取得手段と、

生成された前記共有鍵を用いて、取得されたコンテンツを暗号化して、暗号化コンテンツを生成する暗号化手段とを備え、

前記送信手段は、さらに、生成された前記暗号化コンテンツを送信する

ことを特徴とする請求の範囲３に記載の共有鍵生成装置。

24. 第３者に知られることなく共有鍵生成装置から共有鍵を受け取る共有鍵復元装置であって、

前記共有鍵生成装置は、シード値を生成し、生成された前記シード値から検証値及び共有鍵を生成し、生成された前記検証値を暗号化して、第１暗号化情報を生成し、生成された前記検証値に基づいて、生成された前記シード値を暗号化して、第２暗号化情報を生成し、生成された前記第１暗号化情報及び前記第２暗号化情報を送信し、

前記共有鍵復元装置は、

前記第１暗号化情報及び前記第２暗号化情報を受信する受信手段と、

受信された前記第１暗号化情報を復号して第１復号検証値を生成する第１復号手段と、

生成された前記第１復号検証値に基づいて、受信された前記第２暗号化情報を復号して、復号シード値を生成する第２復号手段と、

前記共有鍵生成装置と同一の方法により、生成された前記復号シード値から第２復号検証値及び復号共有鍵を生成する共有鍵生成手段と、

生成された前記第１復号検証値及び前記第２復号検証値に基づいて、生成された前記復号共有鍵を出力するか否かを判断する判断手段と、

出力すると判断される場合に、生成された前記復号共有鍵を出力する出力手段と

を備えることを特徴とする共有鍵復元装置。

25. 前記共有鍵生成装置は、公開鍵を取得し、取得された前記公開鍵を用いて、前記検証値に公開鍵暗号化アルゴリズムを施して前記第１暗号化情報を生成し、

前記第１復号手段は、

前記公開鍵に対応する秘密鍵を取得する秘密鍵取得部と、

取得された前記秘密鍵を用いて、受信した前記第１暗号化情報に、前記公開鍵暗号化アルゴリズムに対応する公開鍵復号アルゴリズムを施して前記第１復号検証値を生成する公開鍵復号部と含む

ことを特徴とする請求の範囲24に記載の共有鍵復元装置。

26. 前記公開鍵暗号化アルゴリズム及び前記公開鍵復号アルゴリズムは、ＮＴＲＵ暗号方式によるものであり、

前記共有鍵生成装置は、前記公開鍵として、ＮＴＲＵ暗号方式の鍵生成アルゴリズムにより生成された公開鍵多項式を取得し、前記検証値から検証値多項式を生成し、ブラインド値を生成し、生成した前記ブラインド値からブラインド値多項式を生成し、ＮＴＲＵ暗号方式の暗号化アルゴリズムにより、前記公開鍵多項式を鍵として用い、前記検証値多項式を攪乱するために前記ブラインド値多項式を用いて、前記検証値多項式を暗号化して、多項式としての前記第１暗号化情報を生成し、

前記受信手段は、多項式としての前記第１暗号化情報を受信し、

前記秘密鍵取得部は、前記秘密鍵として、ＮＴＲＵ暗号方式の鍵生成アルゴリズムにより生成された秘密鍵多項式を取得し、

前記公開鍵復号部は、ＮＴＲＵ暗号方式の前記暗号化アルゴリズムに対応する復号アルゴリズムにより、前記秘密鍵多項式を鍵として用いて、多項式としての前記第１暗号化情報を復号して、復号検証値多項式を生成し、生成した前記復号検証値多項式から前記第１復号検証値を生成する

ことを特徴とする請求の範囲25に記載の共有鍵復元装置。

27. 前記共有鍵生成装置は、前記検証値に一方向性関数を施して関数値を生成し、生成した前記関数値を用いて、前記シード値に暗号化アルゴリズムを施して前記第２暗号化情報を生成し、

前記第２復号手段は、生成された前記第１復号検証値に、前記一方向性関数を施して復号関数値を生成し、生成した前記復号関数値を用いて、受信された前記第２暗号化情報に、前記暗号化アルゴリズムに対応する復号アルゴリズムを施して前記復号シード値を生成する

ことを特徴とする請求の範囲24に記載の共有鍵復元装置。

28. 前記共有鍵生成装置は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして排他的論理和を施すことにより、前記第２暗号化情報を生成し、

前記第２復号手段は、生成した前記復号関数値と前記第２暗号化情報とに、前記復号アルゴリズムとして排他的論理和を施すことにより、前記復号シード値を生成する

ことを特徴とする請求の範囲 27 に記載の共有鍵復元装置。

29. 前記共有鍵生成装置は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして共通鍵暗号化アルゴリズムを施すことにより、前記第２暗号化情報を生成し、

前記第２復号手段は、生成した前記復号関数値と前記第２暗号化情報とに、前記復号アルゴリズムとして、前記共通鍵暗号化アルゴリズムに対応する共通鍵復号アルゴリズムを施すことにより、前記復号シード値を生成する

ことを特徴とする請求の範囲 27 に記載の共有鍵復元装置。

30. 前記共有鍵生成装置は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして加算を施すことにより、前記第２暗号化情報を生成し、

前記第２復号手段は、生成した前記復号関数値と前記第２暗号化情報とに、前記復号アルゴリズムとして、減算を施すことにより、前記復号シード値を生成する

ことを特徴とする請求の範囲 27 に記載の共有鍵復元装置。

31. 前記共有鍵生成装置は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして乗算を施すことにより、前記第２暗号化情報を生成し、

前記第２復号手段は、生成した前記復号関数値と前記第２暗号化情報とに、前記復号アルゴリズムとして、除算を施すことにより、前記復号シード値を生成する

ことを特徴とする請求の範囲 27 に記載の共有鍵復元装置。

32. 前記共有鍵生成装置は、前記検証値に、前記一方向性関数としてハッシュ関数を施して前記関数値を生成し、

前記第２復号手段は、生成された前記第１復号検証値に、前記一方向性関数として前記ハッシュ関数を施して前記復号関数値を生成する

ことを特徴とする請求の範囲 27 に記載の共有鍵復元装置。

33. 前記共有鍵生成装置は、前記検証値を用いて、前記シード値に暗号化アルゴリズムを施して第２暗号化情報を生成し、

前記第２復号手段は、生成された前記第１復号検証値を用いて、前記第２暗号化情報に、前記暗号化アルゴリズムに対応する復号アルゴリズムを施して、前記復号シード値を生成する

ことを特徴とする請求の範囲 24 に記載の共有鍵復元装置。

34. 前記共有鍵生成装置は、前記検証値及び前記第１暗号化情報を用いて、前記シード値を暗号化し、

前記第２復号手段は、生成された前記第１復号検証値及び受信された前記第１暗号化情報を用いて、前記第２暗号化情報を復号して前記復号シード値を生成する

ことを特徴とする請求の範囲24に記載の共有鍵復元装置。

35. 前記共有鍵生成装置は、前記検証値及び前記第１暗号化情報に一方向性関数を施して関数値を生成し、生成した前記関数値を用いて、前記シード値に暗号化アルゴリズムを施して前記第２暗号化情報を生成し、

前記第２復号手段は、前記第１復号検証値及び前記第１暗号化情報に前記一方向性関数を施して復号関数値を生成し、生成した前記復号関数値を用いて、前記第２暗号化情報に、前記暗号化アルゴリズムに対応する復号アルゴリズムを施して、前記復号シード値を生成する

ことを特徴とする請求の範囲34に記載の共有鍵復元装置。

36. 前記共有鍵生成装置は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして排他的論理和を施すことにより、前記第２暗号化情報を生成し、

前記第２復号手段は、前記復号関数値及び前記第２暗号化情報に、前記復号アルゴリズムとして、排他的論理和を施すことにより、前記復号シード値を生成する

ことを特徴とする請求の範囲35に記載の共有鍵復元装置。

37. 前記共有鍵生成装置は、前記シード値に一方向性関数を施して関数値を生成し、生成した前記関数値から前記検証値及び前記共有鍵を生成し、

前記共有鍵生成手段は、生成された前記復号シード値に、前記一方向性関数を施して復号関数値を生成し、生成した前記復号関数値から前記第２復号検証値及び前記復号共有鍵を生成する

ことを特徴とする請求の範囲24に記載の共有鍵復元装置。

38. 前記共有鍵生成装置は、前記シード値に、前記一方向性関数として、ハッシュ関数を施して前記関数値を生成し、

前記共有鍵生成手段は、生成された前記復号シード値に、前記一方向性関数として、前記ハッシュ関数を施して前記復号関数値を生成する

ことを特徴とする請求の範囲37に記載の共有鍵復元装置。

39. 前記共有鍵生成装置は、生成された前記関数値の一部を前記検証値とし、他の一部を前記共有鍵とすることにより、前記検証値及び前記共有鍵を生成し、

前記共有鍵生成手段は、生成された前記復号関数値の一部を前記第２復号検証値とし、他の一部を前記復号共有鍵とすることにより、前記第２復号検証値及び前記復号共有鍵を生成する

ことを特徴とする請求の範囲37に記載の共有鍵復元装置。

40. 前記共有鍵生成装置は、前記シード値に一方向性関数を施して関数値を生成し、生成した前記関数値から前記検証値、前記共有鍵及びブラインド値を生成し、公開鍵を取得し、取得された前記公開鍵及び生成された前記ブラインド値を用いて、前記検証値に公開鍵暗号化アルゴリズムを施して前記第１暗号化情報を生成し、

前記共有鍵生成手段は、生成された前記復号シード値に、前記一方向性関数を施して復号関数値を生成し、生成した前記復号関数値から前記第２復号検証値、前記復号共有鍵及び復号ブラインド値を生成する

ことを特徴とする請求の範囲 24 に記載の共有鍵復元装置。

41. 前記共有鍵生成装置は、公開鍵を取得し、取得された前記公開鍵及び生成された前記ブラインド値を用いて、前記検証値に公開鍵暗号化アルゴリズムを施して前記第１暗号化情報を生成し、

前記判断手段は、前記第１復号検証値及び前記第２復号検証値に基づく前記判断に代えて、

前記公開鍵を取得する公開鍵取得部と、

取得された前記公開鍵及び生成された前記復号ブラインド値を用いて、生成された前記第１復号検証値又は前記第２復号検証値に前記公開鍵暗号化アルゴリズムを施して再暗号化情報を生成する再暗号化部と、

受信された前記第１暗号化情報及び生成された前記再暗号化情報に基づいて、生成された前記復号共有鍵を出力するか否かを判断する判断部とを備える

ことを特徴とする請求の範囲 40 に記載の共有鍵復元装置。

42. 前記判断部は、前記第１暗号化情報と前記再暗号化情報とを比較し、前記第１暗号化情報と前記再暗号化情報とが一致する場合に、前記復号共有鍵を出力すると判断する

ことを特徴とする請求の範囲 41 に記載の共有鍵復元装置。

43. 前記公開鍵暗号化アルゴリズムは、ＮＴＲＵ暗号方式によるものであり、

前記共有鍵生成装置は、前記公開鍵として、ＮＴＲＵ暗号方式の鍵生成アルゴリズムにより生成された公開鍵多項式を取得し、前記検証値から検証値多項式を生成し、前記ブラインド値からブラインド値多項式を生成し、ＮＴＲＵ暗号方式の暗号化アルゴリズムにより、前記公開鍵多項式を鍵として用い、前記検証値多項式を攪乱するために前記ブラインド値多項式を用いて、前記検証値多項式を暗号化して、多項式としての前記第１暗号化情報を生成し、

前記公開鍵取得部は、前記公開鍵多項式を取得し、

前記再暗号化部は、前記第２復号検証値から復号検証値多項式を生成し、前記復号ブラインド値から復号ブラインド値多項式を生成し、ＮＴＲＵ暗号方式の暗号化アルゴリズムにより、前記公開鍵多項式を鍵として用い、前記復号検証値多項式を攪乱するために前記復号ブラインド値多項式を用いて、前記復号検証値多項式を暗号化して、多項式としての前記再暗号化情報を生成する

ことを特徴とする請求の範囲 41 に記載の共有鍵復元装置。

44. 前記判断手段は、前記第１復号検証値と前記第２復号検証値とを比較し、一致する場合に、前記復号共有鍵を出力すると判断する

ことを特徴とする請求の範囲 24 に記載の共有鍵復元装置。

45. 前記共有鍵生成装置は、さらに、コンテンツを取得し、生成された前記共有鍵を用いて、取得されたコンテンツを暗号化して、暗号化コンテンツを生成し、生成された前記暗号化コンテンツを送信し、

前記受信手段は、さらに、前記暗号化コンテンツを受信し、

前記共有鍵復元装置は、さらに、

出力された前記復号共有鍵を用いて、受信された前記暗号化コンテンツを復号して、復号コンテンツを生成する復号手段と、

生成された復号コンテンツを出力する出力手段とを備える

ことを特徴とする請求の範囲２４に記載の共有鍵復元装置。

46. 第３者に知られることなく共有鍵を相手の装置へ伝える共有鍵生成装置で用いられる共有鍵生成方法であって、

シード値を生成するシード値生成ステップと、

生成された前記シード値から検証値及び共有鍵を生成する共有鍵生成ステップと、

生成された前記検証値を暗号化して、第１暗号化情報を生成する第１暗号化ステップと、

生成された前記検証値に基づいて、生成された前記シード値を暗号化して、第２暗号化情報を生成する第２暗号化ステップと、

生成された前記第１暗号化情報及び前記第２暗号化情報を送信する送信ステップと

を含むことを特徴とする共有鍵生成方法。

47. 第３者に知られることなく共有鍵を相手の装置へ伝える共有鍵生成装置で用いられる共有鍵生成プログラムであって、

シード値を生成するシード値生成ステップと、

生成された前記シード値から検証値及び共有鍵を生成する共有鍵生成ステップと、

生成された前記検証値を暗号化して、第１暗号化情報を生成する第１暗号化ステップと、

生成された前記検証値に基づいて、生成された前記シード値を暗号化して、第２暗号化情報を生成する第２暗号化ステップと、

生成された前記第１暗号化情報及び前記第２暗号化情報を送信する送信ステップと

を含むことを特徴とする共有鍵生成プログラム。

48. 前記共有鍵生成プログラムは、コンピュータ読み取り可能な記録媒体に記録されている

ことを特徴とする請求の範囲４８に記載の共有鍵生成プログラム。

49. 第３者に知られることなく共有鍵生成装置から共有鍵を受け取る共有鍵復元装置で用いられる共有鍵復元方法であって、

前記共有鍵生成装置は、シード値を生成し、生成された前記シード値から検証値及び共有鍵を生成し、生成された前記検証値を暗号化して、第１暗号化情報を生成し、生成された前記検証値に基づいて、生成された前記シード値を暗号化して、第２暗号化情報を生成し、生

成された前記第１暗号化情報及び前記第２暗号化情報を送信し、

前記共有鍵復元方法は、

前記第１暗号化情報及び前記第２暗号化情報を受信する受信ステップと、

受信された前記第１暗号化情報を復号して第１復号検証値を生成する第１復号ステップと、

生成された前記第１復号検証値に基づいて、受信された前記第２暗号化情報を復号して、復号シード値を生成する第２復号ステップと、

前記共有鍵生成装置と同一の方法により、生成された前記復号シード値から第２復号検証値及び復号共有鍵を生成する共有鍵生成ステップと、

生成された前記第１復号検証値及び前記第２復号検証値に基づいて、生成された前記復号共有鍵を出力するか否かを判断する判断ステップと、

出力すると判断される場合に、生成された前記復号共有鍵を出力する出力ステップと

を含むことを特徴とする共有鍵復元方法。

50. 第３者に知られることなく共有鍵生成装置から共有鍵を受け取る共有鍵復元装置で用いられる共有鍵復元プログラムであって、

前記共有鍵生成装置は、シード値を生成し、生成された前記シード値から検証値及び共有鍵を生成し、生成された前記検証値を暗号化して、第１暗号化情報を生成し、生成された前記検証値に基づいて、生成された前記シード値を暗号化して、第２暗号化情報を生成し、生成された前記第１暗号化情報及び前記第２暗号化情報を送信し、

前記共有鍵復元プログラムは、

前記第１暗号化情報及び前記第２暗号化情報を受信する受信ステップと、

受信された前記第１暗号化情報を復号して第１復号検証値を生成する第１復号ステップと、

生成された前記第１復号検証値に基づいて、受信された前記第２暗号化情報を復号して、復号シード値を生成する第２復号ステップと、

前記共有鍵生成装置と同一の方法により、生成された前記復号シード値から第２復号検証値及び復号共有鍵を生成する共有鍵生成ステップと、

生成された前記第１復号検証値及び前記第２復号検証値に基づいて、生成された前記復号共有鍵を出力するか否かを判断する判断ステップと、

出力すると判断される場合に、生成された前記復号共有鍵を出力する出力ステップと

を含むことを特徴とする共有鍵復元プログラム。

51. 前記共有鍵復元プログラムは、コンピュータ読み取り可能な記録媒体に記録されていることを特徴とする請求の範囲５０に記載の共有鍵復元プログラム。

【ABSTRACT OF DISCLOSURE】

暗号装置と復号装置との間で異なる鍵の導出を防止するコンテンツ配信システムを提供する。

暗号装置 110d の乱数生成部 112d は、乱数 s を生成し、第 1 関数部 113d は、乱数 s の関数値 G(s)を生成し、関数値 G(s)から検証値 a と共有鍵 K を生成し、暗号化部 114d は、公開鍵多項式 h を用いて検証値 a の第 1 暗号文 c1 を生成し、第 2 関数部 115d は、検証値 a と第 1 暗号文 c1 の関数値 H(a,c1)を生成し、乱数マスク部 116d は、第 2 暗号文 c2=s xor H(a,c1)を生成する。

復号装置 120d の復号化部 123d は、秘密鍵多項式 f を用いて、第 1 暗号文 c1 を復号して復号検証値 a'を生成し、第 3 関数部 124d は、検証値 a'と第 1 暗号文 c1 の関数値 H(a',c1)を生成し、乱数マスク除去部 125d は、復号乱数 s'=c2 xor H(a',c1)を生成し、第 4 関数部 126d は、復号乱数 s'のハッシュ関数値 G(s')を生成し、関数値 G(s')から検証値 a"と共有鍵 K'を生成し、比較部 127d は、復号検証値 a'と検証値 a"が等しければ、共有鍵 K'を出力する。

（選択図　図１６）